PROBLEM SETS
MONSOON 2025: DISCRETE MATHEMATICS (CS-1110/ MAT-2203-1)

GAURAV BHATNAGAR

Problem solving in Discrete Math

To become good in the subject, you have to do many problems.

(1) For the quizzes, mark corrections or redo the problems as required.
(2) In addition, try the problems I give in class. (I have included them here.)
(3) These problems are to be tried on your own for as long as you possibly can, and then discussed with friends. Learning mathematics is an activity best done as a team. Hearing the words repeatedly, even if in your own voice, helps in absorbing the material.
(4) Increase your stamina and staying power of trying a problem for at-least half-an-hour before giving up and asking someone, or looking it up.
(5) Do not keep trying more than one or two problems for longer than the weekend.
(6) After doing the problem, spend some time in writing your solution neatly in a manner that your argument is clear. If you see your solution after a year, will you understand what you have done? Even if you find out the solution from someone else, write on your own.
(7) You may show your solutions to the TAs and the TF and ask them informally whether it is correct.
(8) You can upload a scanned copy to ChatGPT and ask it to grade and make suggestions (Slightly risky, but may be better than most TAs).
(9) Write code on your own. Then use Chat GPT to find out what you did wrong and can do better. All code written by Chat GPT (or any open AI) has to be tested a bit.
(10) In DS sessions, plan to present a problem if called upon (groups can present too).
(11) These problems will show up in the Quizzes/midterms/final. It may be impossible to do them there if you have not tried them earlier.

1. Problem Set 1

First steps with induction ($n = 1, 2, 3, \dots$)!

Problem 1. Prove the following using the Principle of Mathematical Induction. Some sample problems/solutions are available in my book Experience Mathematics (available here), on pg. 4. Follow this book's way of writing the solutions (rather than how we did in class). Since this is such an important technique, let us target doing 100 proofs by induction this semester!
For each of the following, first verify the two sides are equal for $n = 0, 1, 2, 3$ (if applicable) and then give a proof by induction.

(i.) $1 + 3 + 5 + \cdots + (2k - 1) = n^2$.

(ii.) $T(n) := \sum_{k=0}^{n} k = \dfrac{n(n+1)}{2}$. The $T(n)$ are called triangular numbers. Can you tell why?

(iii.) $\sum_{k=0}^{n} k^2 = \dfrac{n(n+1/2)(n+1)}{3}$.

(iv.) $\sum_{k=0}^{n} k^3 = \left(\dfrac{n(n+1)}{2}\right)^2$.

(v.) $\sum_{k=0}^{n} q^k = \dfrac{1-q^{n+1}}{1-q}$.

(vi.) For $m = 0, 1, 2, \ldots$

$$\sum_{k=1}^{n} k(k+1)\cdots(k+m-1) = \frac{1}{m+1}\left(n(n+1)\cdots(n+m)\right).$$

Here we take m fixed, and do the induction on n. Write down what the statement means for $m = 0, 1, 2, 3$.

(vii.) Again, write down the statement first for $m = 1, 2, 3$ and then prove by induction on n (for a fixed m).

$$\sum_{k=1}^{n} \frac{1}{k(k+1)\cdots(k+m)} = \frac{1}{m}\left(\frac{1}{m!} - \frac{1}{(n+1)(n+2)\cdots(n+m)}\right),$$

for $m = 1, 2, 3, \ldots$.

Getting familiar with objects.

Problem 2 (SS)**.** Define

$$A_1 = \{1, 2, 3, 4, 5, 6\}$$
$$A_2 = \{2, 4, 6, 8, 10\},$$
$$A_3 = \{2, 3, 5, 7, 11, 13, 17\}$$

in the universe

$$X = \{1, 2, 3, \ldots, , 19, 20\}.$$

For $1 \leq i, j \leq 3$, list out the following sets:

(a.) $A_i \cap A_j$
(b.) $A_i \cup A_j$
(c.) A_i^c
(d.) $A_i \setminus A_j$.

Remark 1. Problems marked SS are taken from Professor Sagar Shrivastava's notes from another course.

Problem 3. List all subsets of I_5.

Problem 4. List all elements of $I_3 \times I_4$.

Problem 5. List all functions from I_3 to I_2. Which of these are injective, and which are subjective? Can they be bijective?

Problem 6. List all permutations on 4 letters.

Problem 7. Represent the following concepts using Venn diagrams.

(a.) $A \subset B$.
(b.) $A \cup B$.
(c.) $A \cap B$.
(d.) $A \setminus B$. (Recall that $A \setminus B$ consists of the elements in A but not in B.)
(e.) A^c.

Sets and the beginning of logical thinking.

Problem 8. The following are statements about sets. Make Venn diagrams to 'prove by pictures'.

(a.) If A is a subset of B and B is a subset of C, then A is a subset of C.
(b.) If $B \subset A$, then $A \cup B = A$; and, its converse. (The converse of 'If P then Q' is 'If Q then P'.)
(c.) If $B \subset A$, then for any set C both $B \cup C \subset A \cup C$ and $B \cap C \subset A \cap C$.
(d.) DeMorgans' Laws
   (i) $(A \cap B)^c = A^c \cup B^c$.
   (ii) $(A \cup B)^c = A^c \cap B^c$.
(e.) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
(f.) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
(g.) $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$. (This is called the **symmetric difference** of A and B.)

Problem 9 (SS)**.** Each of the following statements about subsets of a set Ω is FALSE. Draw a Venn diagram to represent the situation being described. In each case, show that the assertion is false by finding a suitable example of the sets.

(1) For all A, B, and C, if $A \not\subseteq B$ and $B \not\subseteq C$ then $A \not\subseteq C$.
(2) For all sets A, B and $C, (A \cup B) \cap C = A \cup (B \cap C)$.
(3) For all sets A, B and $C, (A \backslash B) \cup (C \backslash B) = A \backslash (B \cup C)$.
(4) For all A, B and C, if $A \cup C \subseteq B \cup C$ and $A \cap C \subseteq B \cap C$ then $A = B$.
(5) For all A, B and C, if $A \cup C = B \cup C$ then $A = B$.

Getting a sense of big numbers.

Problem 10. The story goes that the King wishes to reward the inventor of chess, because it is such a nice game and keeps so many people entertained. He asks the inventor what reward he wants. The inventor says: "I want 1 grain of wheat for the first square of the chess board, 2 for the second, 4 for the third, and so on." "This sounds like a very small demand," says the King. He gets angry, that the inventor has asked for so little. "Since you did not respect me to ask for something big, I will order you to be killed." "Wait, your majesty", says the inventor. "First give me what I want, then you can kill me if you find that I asked for too little." Your task:

- Calculate the number of wheat grains asked by the inventor for his reward.
- Lets say a 1000 kg of wheat in a year is enough for a family. It fits in one gunny sack. Calculate how many such sacks will contain this much of wheat.
- How big a building is required for storing these?

You may need to make some assumptions about the weight of an average grain.

Problem 11. Let

$$n! = 1 \times 2 \times 3 \times 4 \times \cdots \times n.$$

We define $0! := 1$.
Calculate (by hand) $n!$ for $n = 0, 1, 2, 3, 4, 5, 6, 7$. Write a code to calculate $n!$ is read **n factorial**. Calculate upto 100! (We take $0! = 1$.)

– You need to use recursion.
– If the inventor had asked for 64! grains of wheat, then how many grains of wheat are required? Do calculations as above and compare the two numbers.

2. Problem Set 2

Understanding the definitions and theorems discussed in the lecture. Each of the 'proof problems' are one or two line arguments.

Problem 12. Prove the following. These properties show that divisibility is a *partial order* on $\mathbb{N}$. In the following, $a, b, c \in \mathbb{N}$.

(i.) $a \mid a$ for all a.
(ii.) If $a \mid b$ and $b \mid a$, then $a = b$.
(iii.) If $a \mid b$ and $b \mid c$, then $a \mid c$.

It is a *partial* order, because all pairs a and b are not comparable in this way. For example, 3 and 5 are not comparable, but $3 \mid 9$. As an example, work out the order relations for all divisors of 24. Make a diagram to represent the relations.

Problem 13. Show that the well-ordering principle (WOP) implies the Principle of Mathematical Induction (PMI).

Problem 14. Find q and r when 514229 is divided by 317811. Suppose the remainder is r_1. Repeat the process with 317811 and r_1, and get remainder r_2. Then repeat for r_1 and r_2, and so on, until you can go no further.

Problem 15.

(a.) List all the primes upto 100 using the Eratosthenes Sieve.
(b.) Let n be a number. Argue that if n is not prime then it is divisible by a prime p such that $p \leq \sqrt{n}$. What does this tell you about Eratosthenes sieve?

Problem 16. Make the addition and multiplication tables for $\mathbb{Z}_6$.

Problem 17. List all invertible and non-invertible elements in $\mathbb{Z}_{24}$.

Problem 18. List all divisors of numbers from 2 to 25. Can you look at a number and predict the number of its divisors?

Problem 19. Let $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$, and a', b' be integers such that

$$a \equiv a' \pmod{m} \text{ and } b \equiv b' \pmod{m}.$$

Then show that:

(i.) $a + b \equiv a' + b' \pmod{m}$.
(ii.) $ab \equiv a'b' \pmod{m}$.

Problem 20. Which of the field axioms work for $\mathbb{Z}$ with $+$ and $\cdot$ as operations? The integers are a prototypical example of an algebraic structure called the *ring*.

Problem 21. Let $\mathbb{F}$ be a field.

(a.) Show that $0 \times a = 0$ for any a in $\mathbb{F}$.
(b.) Show that the linear equation $ax + b = c$ has a solution (for x) provided $a \neq 0$. (Find the solution in $\mathbb{F}$.)

Some numerical experimentation.

Problem 22. Solve the following congruence equations. If there is no solution, say so, and explain why. You can solve all by trying our values for x from the relevant set $\mathbb{Z}_m$ where solutions lie.

(a.) $3x \equiv 1 \pmod{11}$.
(b.) $x^2 \equiv -1 \pmod{7}$.
(c.) $4x \equiv 1 \pmod{7}$.
(d.) $4x \equiv 1 \pmod{6}$.
(e.) $7x \equiv 1 \pmod{18}$.
(f.) $8x \equiv 1 \pmod{18}$.

Problem 23. Calculate the following.

(a.) Calculate $3x \pmod{5}$ for all $x \in \mathbb{Z}_5$. (Your answers should be in $\mathbb{Z}_5$.)
(b.) Calculate $3x \pmod{7}$ for all $x \in \mathbb{Z}_7$.
(c.) Calculate $3x \pmod{8}$ for all $x \in \mathbb{Z}_8$.
(d.) Calculate $3x \pmod{9}$ for all $x \in \mathbb{Z}_9$.

Problem 24. Calculate the powers $a, a^2, \ldots \pmod{m}$, for given a and m.

(a.) $a = 1, m = 5$.
(b.) $a = 2, m = 5$.
(c.) $a = 3, m = 5$.
(d.) $a = 4, m = 5$.
(e.) $a = 3, m = 7$.
(f.) $a = 3, m = 8$.
(g.) $a = 3, m = 9$.

Problem 25. Do the above numerical experimentation problems using Sage.

Abstracting out (some of) what is important.

Problem 26. Let p be a prime and $1 < a < p$.

(a.) Prove that: $ax \equiv b \pmod p$, regarded as an equation of x, has a solution, for any integer b.
(b.) Prove that: if $ax \equiv ay \pmod p$, then $x \equiv y \pmod p$.
(c.) Argue that if $x \not\equiv y \pmod p$, then $ax \not\equiv ay \pmod p$.
(d.) Argue from the above that for a fixed a, where $0 < a < p$, the set

$$\{ax \mid x \in \mathbb{Z}_p\} = \mathbb{Z}_p;$$

that is, the list

$$a \cdot 0, a \cdot 1, \ldots, a \cdot (p-1) \pmod p$$

is a reordering of

$$0, 1, \ldots, p-1.$$

3. Problem Set 3

Logical Puzzles.

Problem 27. Do Puzzles 26–46 of Raymond Smullyan's book *What is the name of this book*. Make sure (after your solution) to read Smullyan's solutions and understand them. Using truth tables is not a good idea. Just argue verbally. That will be more useful to you in the future.

Understanding the theorems of the lectures.

Problem 28. The problem from the quiz.

(a.) State the well ordering principle for natural numbers.
(b.) A number is *interesting*, if it has some property which distinguishes it from other numbers. Show that the set S of uninteresting numbers is empty.

This problem shows every number is interesting!

Problem 29. List the elements of $\mathbb{Z}_{10}^*$, the set of units (invertible elements) of $\mathbb{Z}_{10}$. Make the multiplication table for all of these. What axioms does this number system satisfy, with respect to multiplication? Do the same for $\mathbb{Z}_7^*$.

Problem 30. Find $\varphi(n)$ for $n = 1, 2, \ldots, 13$.

Problem 31. The Fibonacci sequence is defined by: $f_0 = 0$, $f_1 = 1$ and $f_{n+1} = f_n + f_{n-1}$. Write down f_n for $n = 0, 1, \ldots, 5$. Show that $(f_{n+1}, f_n) = 1$ for $n > 1$.

Problem 32. Let $(a, b) = d$, and $c > 0$. Show that $(ac, bc) = dc$.

Problem 33.

(1) Find the inverse of 2 in $\mathbb{Z}_7$, $\mathbb{Z}_{11}$ and $\mathbb{Z}_{13}$. Generalize to find the inverse of $2 \pmod{p}$ for any prime p.
(2) Given that 200003 is a prime, find the remainder when 200000! is divided by 200003.

Problem 34. If p is an odd prime (so $p > 2$), then prove that:

$$1^2 \cdot 3^2 \cdot 5^2 \cdot (p-2)^2 \equiv (-1)^{(p+1)/2} \equiv 2^2 \cdot 4^2 \cdot 6^2 \cdot (p-1)^2 \pmod{p}.$$

Problem 35. Let $n \in \mathbb{N}$.

(a.) Show that $k \nmid n! + 1$ for all $k = 2, 3, \ldots, n$.
(b.) Show that the gcd $(n! + 1, (n+1)! + 1) = 1$.

Problem 36. These are to be done by hand, but you can check your answer by sage.

(a.) Find the remainder when 17^{51} is divided by 144.
(b.) Find the remainder when 2023^{2023} is divided by 31.

Problem 37. Some problems to remind you of prime factorization that you learnt in grade school.

(1) Factor 198 as a product of primes. Write the factors in **standard form**; that is, write the primes in increasing order so you get an expression of the form
$$p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$
where p_1, p_2, …, p_k are the distinct primes dividing 198, and $a_i > 0$.
(2) Express 98 as a product of primes in standard form.
(3) Express 350 as a product of primes in standard form.

Check your answers using Sage.

Theorem 1 (Fundamental Theorem of Arithmetic)**.** *A number can be expressed in only one way as a product of primes in standard form; that is, apart from reordering the primes, there is only one way of expressing a number as a product of primes.*

Problem 38. The following steps outline a proof of this theorem. If you use a proposition from the lectures, state it.

(a.) Let n be a number, and let S be its set of divisors bigger than 1. Show that the least element of S has to be a prime p which divides n.
(b.) Argue that any number can be written as a product of primes.
(c.) Show that any number n can be written in the form
$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

where p_1, p_2, …, p_k are the primes dividing n and $a_i > 0$.

(d.) Suppose $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, and $n = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$, where the p_i's and q_i's are primes and a_i's and b_i's natural numbers. Here p_i's are distinct and q_i's are distinct. Show that $p_1 = q_j$ for some j.

(e.) Suppose $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, and $n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, where the p_i's are distinct primes. Show that $a_1 = b_1$.

(f.) Use the above to complete the proof of Theorem 1.

Definition 2. *Let a and b be two numbers. The* **least common multiple** *of a and b, which we will denote by $[a, b]$ or $\mathrm{lcm}(a, b)$, is the number m such that:*

(i.) $a \mid m$ and $b \mid m$.
(ii.) m is the smallest number with this property.

Problem 39. Find $[98, 350]$.

Problem 40 (Grade school technique to find GCD and LCM)**.**

(a.) Let $m = p^3 q^2 r^7$ and $m = p^2 q^5 s^3$, where p, q, r, s are distinct prime numbers. What is the largest power of p that divides both n and m?

(b.) What is the smallest power of q that a common multiple of n and m must have?

(c.) Let $n = 13^5 17^2 23^{12}$ and $n = 3^5 11^{12} 13^2$. Find (n, m) and $[n, m]$.

Set theory and logic.

Problem 41. Prove the following statements, if not already proved in lecture. For those marked with *, give detailed proofs following the model of the lecture, to explain ideas of logic involved. Show your proofs to Chat GPT and ask it to give feedback.

(a.) If A is a subset of B and B is a subset of C, then A is a subset of C.
(b.) If $B \subset A$, then $A \cap B = B$; and, its converse.*
(c.) If $B \subset A$, then for any set C both $B \cup C \subset A \cup C$ and $B \cap C \subset A \cap C$.
(d.) DeMorgans' Laws
  (i) $(A \cap B)^c = A^c \cup B^c$.
  (ii) $(A \cup B)^c = A^c \cap B^c$.
(e.) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
(f.) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.*
(g.) $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

Add statements from the lectures/previous problems to make a complete list of set theoretic statements for your reference.

Problem 42 (Principle of Inclusion-Exclusion)**.** Let A_1, A_2, A_3, … be sets. Show the following.

(a.) $|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$.

(b.) Prove by induction (for $n = 1, 2, \dots$):

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - \sum_{\substack{1\le i,j\le n\\ i\neq j}} |A_i \cap A_j| + \sum_{\substack{1\le i,j,k\le n\\ i,j,k \text{ distinct}}} |A_i \cap A_j \cap A_k| + \cdots + (-1)^{n+1}|A_1 \cap A_2 \cap \cdots \cap A_n|.$$

We had proved (b.) for $n = 2$ in class. You may use it for the proof of part (a.).

Problem 43 (A sweet problem from my calculus course)**.** There are a 100 guests who came for a Diwali dinner. They ate their fill, but there is always space for a dessert and in fact there were three of them: Ice-cream, Jalebi and Kheer. Every guest ate at-least one of these, some had two, and many had all three. The following report was given by the caterer to the host.

- 73 guests ate Ice-cream, 71 had Jalebi and 67 took Kheer.
- 50 guests ate both the Ice-cream and Jalebi
- 48 had Ice-cream and Kheer
- 45 took a combination of Jalebi and Kheer.

How many had only Ice-cream, how many had only Jalebi and how many only Kheer? (The 73 who ate Ice-cream include people who ate Ice-cream and Jalebi.) Do this using the above, and by making pictures.

Some nice number theory problems. These problems will not appear in a Quiz before the midterm. You may try them for a longer time.

Problem 44.

(1) Show that $13 \mid 2^{70} + 3^{70}$.
(2) Show that $11 \cdot 31 \cdot 61 \mid 20^{15} - 1$.
(3) Show that $61! + 1 \equiv 0 \pmod{71}$.
(4) Show that $63! + 1 \equiv 0 \pmod{71}$.

Problem 45 (Challenge problem)**.** Try this problem for as long as it takes to solve it, to get a sense of Euler's cleverness. Prove that:

$$2^{2^5} + 1 \equiv 0 \pmod{641}.$$

4. Problem Set 4

Engaging with the ideas of the lecture.

Problem 46 (Taylor's theorem)**.** Let $a = \sum_k a_k q^k$ be a formal power series. Let D^k be the kth (formal) derivative, and let $a(0) = a_0$, the constant term. Show, using induction, that for $k = 0, 1, \dots$:

$$a_k = \frac{D^k(a(0))}{k!}.$$

Problem 47. Obtain the formula

$$\frac{1}{1-q} = \sum_{k=0}^{\infty} q^k$$

using Taylor's theorem (for formal power series).

Problem 48. Let $f(q)$ and $g(q)$ be formal power series. Show that if $g(0) = 0$, then $f(g(q))$ is also a formal power series by explaining how to obtain the coefficient of q^m for any m. Use this to obtain the following formal power series expansions.

$$\frac{1}{1+q} = 1 - q + q^2 - q^3 + \cdots$$
$$\frac{1}{1-q^2} = 1 + q^2 + q^4 + q^6 + \cdots .$$

Problem 49. Write the first 7 rows of Pascal's triangle using the three-term recurrence relation for the binomial coefficients.

Problem 50. Prove using the interpretation of binary strings.

(a.) $\binom{n}{k} = 0$ if $k > n$.

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

(c.) $\binom{n}{0} = 1 = \binom{n}{n}$, for $n > 0$. Why is this true for $n = 0$?

(d.) $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$, for $k > 0$.

Problem 51. Let

$$F(n,k) := \frac{n!}{k!(n-k)!}$$

, and $F(n,0) = 1$, $F(n,k) = 0$ for $k > n$. Show that

$$F(n+1,k) = F(n,k-1) + F(n,k).$$

Why does this prove that

$$F(n,k) = \binom{n}{k}.$$

Problem 52. The terminating binomial theorem can be stated as:

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

where

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

(a.) Prove the terminating binomial theorem using induction.

(b.) Implement $I_n = \{1, 2, \ldots, n\}$ as a list in Sage. Write a program/function to list all the subsets of I_n using the Set data structure available in Sage. Use this function to make rows of Pascal's triangle.

Definition 3 (q-rising factorials)**.** *We define $(a;q)_n$ as follows. When $n = 0$, $(a;q)_0 := 1$. For $n > 0$,*

$$(a;q)_n := (1-a)(1-aq)\cdots(1-aq^{n-1}).$$

Note that there are n factors in the product. In this notation, we can state the theorem we proved in Lecture 8 as follows.

Theorem 4 (Non-commutative q-binomial theorem)**.** *Suppose $yx = qxy$ and q commutes with both x and y. Then, for $n = 0, 1, 2, \ldots,$*

$$(x+y)^n = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q x^{n-k} y^k, \tag{4.1}$$

where

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q;q)_n}{(q;q)_k (q;q)_{n-k}}. \tag{4.2}$$

Problem 53. Take (4.1) as the definition of the q-binomial coefficient. This problem outlines the derivation of Formula (4.2).

(a.) Show the following boundary conditions:

$$\begin{bmatrix} n \\ 0 \end{bmatrix}_q = 1, \; \begin{bmatrix} n \\ k \end{bmatrix}_q = 0 \text{ for } k > n \text{ and } \begin{bmatrix} n \\ n \end{bmatrix}_q = 1.$$

(b.) Prove the second equation in the following, for $k > 0$.

$$\begin{bmatrix} n+1 \\ k \end{bmatrix}_q = q^k \begin{bmatrix} n \\ k \end{bmatrix}_q + \begin{bmatrix} n \\ k-1 \end{bmatrix}_q$$

$$\begin{bmatrix} n+1 \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ k \end{bmatrix}_q + q^{n-k+1} \begin{bmatrix} n \\ k-1 \end{bmatrix}_q.$$

We had proved the first one in class.

(c.) Show that, for $k > 0$:

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{1-q^{n+1-k}}{1-q^k} \begin{bmatrix} n \\ k-1 \end{bmatrix}_q.$$

(d.) Show that

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q;q)_n}{(q;q)_k (q;q)_{n-k}}.$$

(e.) Verify this formula using Sage for some values of n, k.
(f.) Show that, for $n > 0$,
$$\lim_{q\to 1} \frac{\left(q^A;q\right)_n}{(1-q)^n} = A(A+1)\cdots(A+n-1).$$
(g.) Show, by taking appropriate limits, that
$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Some further explorations.

Problem 54. Let i be defined by $i^2 = -1$. Define the expressions $\sin x$ and $\cos x$ by:
$$e^{ix} = \cos x + i \sin x,$$
where
$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots .$$
Find the first 4 terms of the series expansion of $\cos x$ and $\sin x$. This is how $\sin x$ and $\cos x$ are defined when x is a complex number, but there we need convergence of series.

Problem 55. Obtain the first ten terms of the following series expansions using Sage.
(a.) $1/1 + x^2$
(b.) $\log(1 + x)$
(c.) $\tan^{-1} x$
Do the same for any functions you have studied.

Problem 56. Find (using sage or by hand), the coefficient of q^{100} in the power series expansion of:
$$\frac{1}{(1-q)(1-q^5)(1-q^{10})(1-q^{25})(1-q^{50})}.$$

Definition 5 (Falling factorials). *Define $P(x, n)$ for $n = 0, 1, \ldots,$ as: $P(x, 0) := 1$, and*
$$P(x, n) := x(x-1)\cdots(x-n+1).$$
Note that there are n terms in the product. Recall that $P(m, n)$ is the number of n permutation on I_m.

Problem 57. Note that $P(x, n)$ is a polynomial in x of degree n and so can be written in the form
$$P(x, n) = \sum_{k=0}^{n} s(n, k)x^k.$$
The coefficients $s(n, k)$ are called the **Stirling numbers of the first kind**.

(1) Show that

$$s(n+1,k) = s(n,k-1) - ns(n,k),$$

and the initial and boundary conditions:

$$s(0,0) = 1; s(n,0) = 0 \text{ for } n > 0; s(n,k) = 0 \text{ for } k > n.$$

(2) Use this to write a Sage program to make a table of $s(n,k)$ for $n, k \leq 10$. (Make a table upto $n, k \leq 5$ by hand first.)

Counting in two different ways. These two problems will help you understand the oldest combinatorial trick in the world.

Remark 2 (Counting in two different ways). Let (A, B) be a pair of sets. Suppose for a given $a \in A$, let

$$U(a) = \{(a,b) : b \in B\},$$

and similarly, for $b \in B$, let

$$V(b) = \{(a,b) : a \in A\}.$$

Then we must have

$$\sum_{a \in A} |U(a)| = \sum_{b \in B} |V(b)|.$$

Both the equalities equal $|A \times B|$. This idea was used in Lecture 2.

Problem 58 (The formula for the binomial coefficient)**.** This problems outlines how to find the formula for binomial coefficients by counting permutations in two different ways. Consider pairs (A, B) where A is a k subset of I_n, and B is a permutation on k-letters. Let $\binom{n}{k}$ be the number of k subsets of I_n. Count in two different ways:

(i.) For fixed k-subset A, how many permutations are there on those k-letters?
(ii.) For a given permutation, how many k-subsets correspond to that permutation?

For both of the above, you need to count the number of pairs (A, B). Use the formula for $P(n,k)$, the number of k-permutations on n-letters found in Lecture 2. Equate the two to obtain the formula for $\binom{n}{k}$ where $0 < k < n$. Check whether the formula works for $k = n$ and $k = 0$.

The following problem requires the definition of a graph.

Definition 6. *A graph G consists of a pair of sets (V, E), where V (the set of vertices) and E (the set of edges) such that each $e \in E$ is a 2-subset $\{v_1, v_2\}$ of V. If an edge $e = \{v_1, v_2\}$, we say e is an edge between the vertices v_1 and v_2. (This is also called an undirected, simple, graph.) Occasionally, we allow extensions of this definition. We allow loops which is an edge with one vertex. The edge set can be a multi-set: two edges between v_1 and v_2 are called parallel edges. We also have directed graphs, where an edge is directed from v_1 to v_2.*

Problem 59. Both the following statements are referred to as the Handshaking Lemma.

(a.) Show that in a large meeting, the number of delegates who shake hands an odd number of times is even.

(b.) Let G be a graph without loops with vertex set $\{v_1, \ldots, v_n\}$. Let d_i be the number of edges incident with v_i. Show that

$$\sum_i d_i = 2|E|.$$

5. Problem Set 5

Some number theory.

Recall that $\varphi(m)$ is the number of elements $a \in \mathbb{Z}_m$ which are relatively prime to m. By a proposition in Lecture 5, a is invertible, so $\varphi(m) = |\mathbb{Z}_m^*|$, the cardinality of $\mathbb{Z}_m^*$.

Problem 60. This is about $\varphi(p^n)$, where p is a prime.

(a.) Explicitly list the elements of $\mathbb{Z}_p^*$. There should be $\varphi(p) = p - 1$ of them.

(b.) In $\mathbb{Z}_{p^2}$, list the elements a such that $(a, p) \neq 1$. How many are there?

(c.) Find $\varphi(p^2)$.

(d.) Prove that $\varphi(p^n) = p^n - p^{n-1}$.

(e.) Find $\varphi(97^2)$ (the midterm problem).

Problem 61 (Euler)**.** Generalize the proof of Fermat's little theorem to show that if $(a, m) = 1$, then

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

Binomial coefficient identities.

Problem 62.

(a.) Prove that, for $n = 0, 1, 2, \ldots$

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

(b.) Prove that for $n \geq 0$:

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = \delta_{n,0} = \begin{cases} 1 & \text{if } n = 0; \\ 0 & \text{if } n > 0. \end{cases}$$

Problem 63. Prove the following binomial coefficient identities.

(a.) $\displaystyle\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$

(b.) Show the Chu–Vandermonde identity:

$$\sum_{k=0}^{j} \binom{n}{k}\binom{m}{j-k} = \binom{m+n}{j}. \tag{5.1}$$

(c.) $\displaystyle \binom{n}{0}\binom{n}{m} + \binom{n}{1}\binom{n}{m+1} + \cdots + \binom{n}{n-m}\binom{n}{n} = \binom{2n}{n-m}.$

Generatingfunctionology.

Problem 64. Find the ordinary generating function of 2^n. This completes one of the examples in Lecture 1.

Problem 65.

(a.) Expand $(1-x)^{1/2}$ using the binomial series upto x^3 term.
(b.) Find the coefficient of x^n for $n = 0, 1, 2, 3$ in the square of the series you have found. This verifies whether you calculated the series correctly.

Problem 66. Calculate the first three terms of $e^{\log(1+x)}$ by hand. (Recall that $f(g(x))$ is defined as a formal power series if $g(0) = 0$.)

Problem 67. Obtain formal power series expansions (using the Binomial series) for the series in Problem 55. You can assume that you can differentiate series term by term (and so also find the anti-derivative). Compare the first 4 terms (for $n = 0, 1, 2, 3$) with the sage output.

Problem 68. Let i be such that $i^2 = -1$. Let $n \in \mathbb{N}_0$. Calculate i^{4n+k}, for $k = 0, 1, 2, 3$.

Problem 69. Consider the formal power series

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots = \sum_{k=0}^{\infty} \frac{x^k}{k!}.$$

(a.) Compute the first ten terms of $e^x e^y$. (Multiply the two series.) Do the first 3 by hand, and the rest using Sage.
(b.) Show that, as formal power series,

$$e^x e^y = e^{x+y}.$$

Problem 70. We define $\cos x$ and $\sin x$ by $e^{ix} = \cos x + i \sin x$. Write down the nth term of each of these series.

6. Problem Set 6

This is a holiday homework and meant to be finished before you return from the break. Holidays are meant for relaxation; do these and relax!

Problem 71. Here is a problem you can give as a challenge to that annoying kid in your family whom you meet over the break!

There are three college students—Arjun, Anmay and Avik—each interested in two subjects. They major in two of the following subjects: Biology, Computer Science, Economics, Mathematics, Psychology and Statistics. Further, no two are interested in the same subject. From the following information, find out both the majors of each one of Arjun, Anmay and Avik.

(a.) The computer scientist says the mathematician should learn how to program computers.
(b.) Both the mathematician and statistician plan to run a half-marathon with Arjun this semester.
(c.) The psychologist insists that the economist pays when they eat together at the snack bar.
(d.) The computer scientist and the psychologist are never in the same class.
(e.) Anmay asks the statistician for help with his homework.
(f.) Avik beats both Anmay and the psychologist at chess.

Hint. You can buy this book (written with my daughter) for the solution of this problem.

Elementary enumeration and basic combinatorial constructs.

Problem 72 (Permutations)**.** There are many ways in which permutations show up. For all the following, show the one-to-one correspondence by means of suitable examples/pictures. (See, for example, Lecture 8 for an example where we communicate 1-to-1 correspondence of paths with binary strings with subsets.)

(1) (Balls into boxes) We can put n balls labelled 1, 2, ..., n into m boxes (labelled 1 to m), where a box can get at most one ball.
(2) (Sampling balls) Suppose there are m balls in an urn. The balls are labelled 1, 2, ..., m. From here n balls are removed, in order, without replacement, to form an n-permutation. Note that the balls are *distinguishable* (since they are labelled), and *order matters*.
(3) (Lists) The set I_m is representative of any set of m symbols. The permutation can be thought of a listing of n of these symbols, represented as $(x_1, x_2, \dots, x_n)$ or simply a string $x_1x_2 \dots x_n$.
(4) (Words) One could have a set of symbols

$$\{y_1, y_2, \dots, y_n\}$$

called an alphabet. An n-permutation is a word $x_1x_2 \dots x_n$, where the x_i are from this alphabet, and are distinct.
(5) (Injective mappings) Consider functions $f : I_n \to I_m$ which are injective (or 1-1). What does the condition 1-1 mean in this approach?

Problem 73 (Subsets)**.** There are many ways in which subsets show up. For all the following, show the one-to-one correspondence by means of suitable examples/pictures.

(1) The alphabet consists of $\{0, 1\}$ and words are of length n, with exactly k 1's.
(2) (Balls in Boxes) We can distribute n labelled balls into two boxes. Exactly k balls are placed in the box labelled 1, and the rest go into the other.
(3) (Sampling balls) Suppose there are n balls in an urn. The balls are labelled 1, 2, ..., n. From here k balls are taken to form a k-subset. The order in which they are sampled is not noted. Note that the balls are *distinguishable* (since they are labelled), and *order does not matter.*
(4) (Combinations) A k-subset T of an n-set S is sometimes called a k-combination without repetitions.
(5) (Binary strings) A k-subset of I_n corresponds to a binary string of length n, with the number of 1's equal to k. (Of course, we could define with exactly k 0's too.)
(6) (Paths) A lattice path in the first quadrant with n steps. Steps are on lattice points, that is, points (x, y) with x, y integers. Each step is a North or East step. The path has exactly k horizontal steps.
(7) Each element of an n-set S may be placed in two categories. Exactly k may be placed in Category 1 and $n - k$ in Category 2. The elements of Category 1 define a k-subset T of S.

Problem 74 (Ordered distributions)**.** List ordered distributions of I_n into m boxes labelled by I_m, in order, for $n = 1, 2, 3, 4$, and $1 \leq m \leq n$. Verify the total number is $(m)_n$ for each of these.

Definition 7 (Multiset)**.** *A* **multiset** *is a set where we allow repetitions. As in sets, the order does not matter. Let A represent a multiset with elements taken from I_m. For each $i \in A$, we have to specify a_i, where*

$$a_i = \#\ \text{of times } i \text{ appears in } A.$$

The multiset A, written as

$$A = \{1^{a_1}, 2^{a_2}, \dots, m^{a_m}\},$$

has a_1 1's, a_2 2's, and so on. The cardinality $|A|$ of the multiset is defined to be

$$|A| := \sum_{i=1}^{m} a_i.$$

Problem 75 (Combinations with repetition)**.** The solutions of the equation

$$x_1 + x_2 + \cdots + x_m = n,$$

where $x_i \geq 0$ are non-negative integers (rather than positive integers). These are called *weak m-compositions.* List weak m-compositions for $n = 3$, $n = 4$, $m = 1, 2, \dots, m$.

The number is given by

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

For the following, show one-to-correspondence with associated objects, by examples, with $n = 3, 4$.

(a.) (Balls in boxes) Suppose n indistinguishable balls are placed into m boxes. You may think of indistinguishable as colored with one color, say red.
(b.) (n-combinations with repetitions) Choose n elements from I_m, repetitions are allowed, and order does not matter. Some authors use the symbol

$$\left(\binom{m}{n}\right)$$

for the number of n-combinations with repetitions. (Note. There is a somewhat confusing interchange of n and m. Take care to understand it.)
(c.) (Sampling with replacement) There are m labelled balls in an urn, with labels 1, 2, ..., m. Withdraw a ball and note its number, and put the ball back. Make n such withdrawals.
(d.) A multiset of cardinality n with elements from I_m.

Problem 76. Let n and m be positive integers. Show that the number of non-negative, integral solutions to the inequalities

$$x_1 + x_2 + \cdots + x_m \leq n$$

is

$$\binom{n+m}{m}.$$

Hint. Convert the inequality into an equality.

Problem 77 (Compositions)**.** Recall that a **composition** of n is an ordered sum of a positive integer into positive integers.

(a.) List all m-compositions of 5, for $m = 0, 1, 2, 3, 4, 5$.
(b.) Illustrate by example that each m-composition of n corresponds to a solution of the equation

$$x_1 + x_2 + \cdots + x_m = n,$$

where each $x_i > 0$ is an integer.
(c.) Obtain the formula for the number of compositions by interpreting them as n unlabelled objects, placed in m labelled boxes, where each box gets at-least one object. Model objects by dots and partition boxes by bars.
(d.) Show (by example) a one-to-one correspondence with subsets of I_{n-1} with $(m-1)$ elements.

Problem 78 (Multinomial coefficients)**.** Recall the multinomial coefficient. Suppose we have m categories C_1, C_2, …, C_m, and the n elements of I_n are placed in these categories with C_i getting exactly k_i elements, with

$$k_1 + k_2 + \cdots + k_m = n.$$

We obtained the formula:

$$\binom{n}{k_1, k_2, \ldots, k_m} = \frac{n!}{k_1!k_2! \cdots k_m!}.$$

For all the following, show the one-to-one correspondence by means of suitable examples/pictures.

(1) (Balls in Boxes) Take n balls labelled 1 through n (and so, distinguishable) and place them into m distinguishable boxes. The boxes represent categories.
(2) (Sampling) In an urn, there are k_1 balls of color 1, k_2 of color 2, …, k_m balls of color m, such that $k_1 + k_2 + \cdots + k_m = n$. Withdraw balls one after the other, and keep track of the colors of the ball in the order they are sampled. The number of such arrangements is given by the multinomial coefficient.
(3) There are k_1 balls of color 1, k_2 of color 2, …, k_m balls of color m, such that $k_1 + k_2 + \cdots + k_m = n$. The number of ways they can be arranged in order is the multinomial coefficient.
(4) (Multiset permutation) Let

$$M = \{1^{k_1}, 2^{k_2}, \ldots, m^{k_m}\}$$

be a multiset with cardinality $|M| = n$, that is, $\sum_i k_i = n$. A permutation of the multiset is a linear listing of the elements where each i comes exactly k_i times in the permutation. For example, the multiset $\{1, 2, 2, 3\}$ has 12 permutations, given by

$$2123, 1223, 1232, 2132, 1322, 2213, 2231, 2321, 2312, 3212, 3122, 3221.$$

Problem 79 (Multinomial Theorem)**.**

(a.) Show, by induction, the multinomial theorem.

$$(x_1 + x_2 + \cdots + x_m)^n = \sum_{\substack{\sum_{j=1}^{m} k_j = n \\ k_1, k_2, \ldots, k_m \geq 0}} \binom{n}{k_1, k_2, \ldots, k_m} x_1^{k_1} x_2^{k_2} \ldots x_m^{k_m}. \tag{6.1}$$

(b.) Show that:

$$\binom{n}{r_1, r_2, \ldots, r_k} = \sum_{i=1}^{k} \binom{n-1}{r_1, \ldots, r_i - 1, \ldots, r_k}.$$

(c.) Go over what we did in the lectures regarding the binomial coefficients. How would you generalize lattice paths and strings to multinomials?

Problem 80 (Set partitions)**.** List all set partitions of I_n, for $n = 0, 1, 2, 3, 4, 5$. Make a table of Stirling numbers $S(n, k)$ by hand and verify that the number matches.

Problem 81. List all equivalence classes of I_3.

Problem 82. List all partitions of n, for $n = 1, 2, \ldots, 6$.

Some exploratory problems. In the following problems, use

$$e^{ix} = \cos x + i \sin x.$$

Problem 83 (de Moivre's formula)**.** Show that, for any $n \in \mathbb{R}$.

$$(\cos x + i \sin x)^n = \cos nx + i \sin nx.$$

Prove this formula using induction for the special case $n = 0, 1, 2, 3, \ldots$ using high-school trigonometric formulas.

Remark 3 (Complex numbers: A very short introduction). Let $z = x + iy$, where x, y are real numbers. We can represent z as (x, y) in the plane. We define the absolute value: $|z| := \sqrt{x^2 + y^2}$. This is the distance of $z = (x, y) = x + iy$ from the origin.

Problem 84 (Roots of unity)**.** Assume now that $\cos x$ and $\sin x$ are the usual functions when x is real. Let $n \in \mathbb{Z}$. Recall the values: $\cos 2n\pi = 1$ and $\sin 2n\pi = 0$ (and other special values). In the following, if you use any previous problem, mention exactly what you used.

(a.) Show that $|e^{ix}| = 1$.
(b.) Show 'the most beautiful formula': $e^{\pi i} + 1 = 0$.
(c.) Show that $e^z = e^x(\cos y + i \sin y)$.
(d.) Show that $e^{z+2n\pi i} = e^z$ for $n \in \mathbb{Z}$. That is, e^z is periodic, with period $2\pi i$.
(e.) Solve the equation $z^n = 1$ for $n = 1, 2, 3$ by hand.
(f.) Solve $z^n = 1$ for $n = 1, \ldots, 10$ by Sage and plot them. Describe your observations.
(g.) Let $z^n = 1$, for $n \in \mathbb{N}$. Then show that

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

(h.) For fixed $n = 1, 2, \ldots,$ consider the set

$$\Omega := \left\{ e^{2k\pi i/n} \mid k = 0, 2, \ldots, n-1 \right\}.$$

Denote $\omega = e^{2\pi i/n}$. Then this set has $1, \omega, \omega^2, \ldots, \omega^{n-1}$. We use the usual multiplication as an operation on this set. Which all algebraic axioms hold for this multiplication? Does this set remind you of anything you have studied so far?

(i.) Let t be such that $(t, n) = 1$. Show that: $\omega_t := \omega^t$ and its powers generate the set Ω, that is:

$$\Omega = \left\{ \omega_t^k \mid k = 0, 1, \ldots, n-1 \right\}.$$

Show that $\omega_t^n = 1$. What all properties of modular arithmetic do you need to show these? State them.

Remark 4. This problem is central to computer science. It is at the heart of the so-called *discrete Fourier transform.* If $z^n = 1$, then z is called an *nth root of unity.* Let ω_t be as above; it is called a *primitive root of unity.* Recall Fermat's little theorem and its generalization by Euler. What do they tell you about roots of unity in $\mathbb{Z}_p$ and $\mathbb{Z}_m$?

Problem 85. (Lots of changes here) This problem is similar to Problem 57. Recall the definition of the rising factorial $(x)_n$, which is a polynomial in x of degree n and so can be written in the form

$$(x)_n = \sum_{k=0}^{n} F(n, k) x^k.$$

The coefficients $F(n, k)$ turn out to be related to the Stirling numbers of the find kind $s(n, k)$:

(1) Show that

$$F(n+1, k) = F(n, k-1) + nF(n, k),$$

and the initial and boundary conditions:

$$F(0, 0) = 1; F(n, 0) = 0 \text{ for } n > 0; F(n, k) = 0 \text{ for } k > n.$$

(2) Show that this recurrence relation and initial and boundary values determine $F(n, k)$.
(3) Show that $F(n, k) = (-1)^{n+k} s(n, k)$.
(4) Use this to write a Sage program to make a table of $s(n, k)$ for $n, k \leq 10$. (Make a table upto $n, k \leq 5$ by hand first.)

Problem 86 (Sage)**.** For all the combinatorial objects mentioned in the course so far, list the first few values by hand, and then until $n = 10$ by using Sage. Do the same for all the special numbers mentioned so far (Fibonacci numbers, binomial coefficients, Stirling numbers of both kinds, Bell numbers).

Problem 87 (Order of sequences)**.** This is a problem from my calculus course, with some extensions. This problem will be useful when studying the speed of algorithms in computer science. In computer science it helps to estimate the number of operations required by an algorithm given the size of the input. Once you have an estimate, such a comparison is useful to predict whether the algorithm is practical or not.

Order the following sequences according to how fast they grow. Draw graphs using Desmos/Sage to guess, and then look at the limit as $n \to \infty$, to draw your conclusions. Justify all your conclusions. In some cases, comparing logs is a good idea. (Since log is an increasing and 1-1 function, if $\log a < \log b$ then $a < b$.) You may need to generate some using Sage for large values to guess the answer.

$$a_n = 1, n^2, 2n+3, n\log n, e^n, 2^n, \log n, (\log n)^2, n^5, H_n := \sum_{k=1}^{n} \frac{1}{k},$$
$$\frac{n}{\log n}, \frac{e^n}{n^3}, \frac{1}{n}, e^{-n}, e^{\log n}, \log(\log n), n!, n^{n/2}, \binom{n}{\lfloor n/2 \rfloor}, b(n), S(n, \lfloor n/2 \rfloor).$$

Use the symbol $f \prec g$ to represent that $f/g \to 0$ as $n \to \infty$. For now, we use $f \equiv g$ if $f/g \to c$ for some constant $c \neq 0$.
Most of these functions go to infinity. We're trying to order them according to 'how fast' they go to infinity.

Ashoka University, Sonipat, Haryana 131029, India
Email address: gaurav.bhatnagar@ashoka.edu.in