MAT202: Introduction to Discrete Mathematics

MAT202: Introduction to Discrete Mathematics

TJ Yusun

University of Toronto Mississauga
Mississauga, ON, Canada

July 16, 2020

Source files: The source files for this document can be found at this git repository. The sources are licensed under the CC-BY-NC-SA 4.0 License.

Edition: Introduction to Discrete Mathematics: September 2020

Website: itdm

Welcome Message

September 2020

Hello all!

My name is ***TJ***, and this semester I will be joining you in your journey to discover and learn about discrete mathematics. I did my PhD at Simon Fraser University, in the area of operations research. You can call me Professor/Prof. Yusun, Dr. Yusun, or simply TJ. My pronouns are he/him/his.

It's been a wild ride this year, and we're only 2/3 of the way through! We have all been affected in different ways by many different events, and it is understandable that you may not be in the optimal mindset to study, especially since you'll be doing this from your homes, dorms, residences. I guess you also miss seeing people, hanging out with your friends, going to the library on campus...I mean, you probably miss waiting for your *Thai Express* order from the Davis Food Court!

I hear you, and I personally would like nothing more than to be able to see your faces in person this Fall term. Unfortunately we've had to make some adjustments, and here we are—meeting each other through words on a screen instead.

In recognition of the unusual position we're all in, I'd like to make a number of commitments to you:

- In all aspects of the course, I will be clear and organized, and reduce as many barriers to your access and learning that I can.
- I will be reasonably available to help you with your learning.
- I will do my best to listen when you speak. Your voices are important to me.
- I will treat you with respect and dignity, and make our class a safe learning environment for you and your peers.

In return, all I ask is that:

- You uphold academic integrity in everything you do.
- You sincerely attempt to engage actively in the course (material, classes, tutorials, and discussions) and submit assessments by their due dates.
- You treat your classmates, TAs and instructor with respect and dignity, and make the class a safe learning environment for everyone.
- You expect to make mistakes, and view them as opportunities to learn and grow.
- You reach out to me and communicate any thoughts or concerns you may have about the course, or anything that you want me to know.

Moreover, there *will* be technology difficulties and failures throughout the term, for both you and me. (In the Winter I had to cancel a class because my internet went out for one whole day.) This is to be expected, and we will manage.

Finally, let me reiterate that *I want you to succeed*, and I will try my best to facilitate this. But also remember that your success depends on the actions you take. We are in this together.

TJ

How to Use This Resource

Read it

Feedback and Acknowledgements

Feedback These notes are being developed by TJ Yusun for the Fall and Winter 2020-2021 offerings of MAT202: Introduction to Discrete Mathematics course at the University of Toronto Mississauga. This is an ongoing project, and so the text may contain errors or typos. Errata will be posted in the Quercus course container for MAT202 as they are found; students are also encouraged to email tj.yusun@utoronto.ca if you find any errors or would like to provide feedback about these notes.

When emailing, please include the following:

- Description of error
- URL of error (if in the online version)
- page number of error (if in the PDF version), and compile date on the front page of the pdf.

Acknowledgements Massive thanks to all the contributors to the PreTeXt system, which was used to produce HTML and PDF outputs of this work.

Contents

Chapter 1

Review of MAT102

The word *discrete* in the title of our course means *separate*; something that is *not smooth*.

In the study of discrete mathematics we will typically concern ourselves with discrete objects such as the integers, graphs, finite and countable sets. (In contrast, excluded from this are objects that may vary continuously, such as those ones covered in trigonometry, calculus, and Euclidean geometry.)

Many of the concepts you learned in your MAT102 course will be useful in MAT202; in this chapter we briefly review some definitions and results, and present some exercises to warm up for the rest of the course! Material in this chapter is based on *MAT102H5 Introduction to Mathematical Proofs* by *Shay Fuchs* [3].

1.1 ▲ Sets and Functions

A **set** is is just a collection of objects (where the order in which the objects are listed does not matter). The following set operations should be familiar to you: intersection $A \cap B$, union $A \cup B$, complement A^c, difference $A \setminus B$, and Cartesian product $A \times B$.

We also recall that proving the set A is a subset of the set B simply necessitates showing that any element of A can also be found in B.

Definition 1.1.1 Set Inclusion and Equality.

If A and B are sets in some universe U, then we say A **is a subset of** B, denoted by $A \subseteq B$, if

$$(\forall x \in U)(x \in A \Rightarrow x \in B).$$

We say that A and B are **equal** as sets if $A \subseteq B$ and $B \subseteq A$ both hold. This means that

$$(\forall x \in U)(x \in A \Leftrightarrow x \in B).$$

Checkpoint 1.1.2 Prove Set Inclusion. Define

$$A = \{k \in \mathbb{Z} : k = 6s + 3 \text{ for some } s \in \mathbb{Z}\}$$

and

$$B = \{m \in \mathbb{Z} : m = 3t \text{ for some } t \in \mathbb{Z}\}.$$

Prove that $A \subseteq B$ holds.

Hint. Pick an arbitrary element in A, call it x. Then you know $x = 6s + 3$ for some integer s. Can you express x in the form $3t$ where t is an integer?

We will use the standard notation for these sets of numbers:

$$\mathbb{N} = \{1, 2, 3, \dots, \}$$
$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$
$$\mathbb{Q} = \left\{\frac{p}{q} : p, q \in \mathbb{Z}\right\}$$
$$\mathbb{R} = (-\infty, \infty), \text{ the set of real numbers.}$$

Intervals of real numbers are denoted by $(a, b), [a, b]$, and other combinations, with $-\infty$ or ∞ as one of both of the endpoints.

Remark 1.1.3

Interval notation is used to refer to sets of real numbers. It is *incorrect*, for instance, to say that $(-2, 4) = \{-1, 0, 1, 2, 3\}$, or that $\{0, 1, 2, 3, \dots\} = [0, \infty)$. Watch your notation!

Definition 1.1.4 Function.

A **function**

$$f : A \to B$$

is a rule that takes elements from its **domain** A and assigns to each one an element from the **codomain** B.

Definition 1.1.5 Injective, surjective, bijective.

A function $f : A \to B$ is

- **injective** if for every $x_1 \neq x_2 \in A$, $f(x_1) \neq f(x_2)$.
- **surjective** if for every $y \in B$, there exists an $x \in A$ so that $f(x) = y$.
- **bijective** if for every $x_1 \neq x_2 \in A$, $f(x_1) \neq f(x_2)$.

Checkpoint 1.1.6 Injective, surjective, bijective, or none? For each function, determine if it is injective, surjective, bijective, or none of these:

(a) $f : \mathbb{R} \to (0, +\infty)$, $f(x) = \sqrt{x^2 + 1}$

(b) $g : \mathbb{N} \to \mathbb{N}$, $g(m) = 3m + 7m^2$

(c) $h : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $h(a, b) = \dfrac{ab(b-1)}{2}$

Definition 1.1.7 Composition.

Given two functions $f : A \to B$ and $g : B \to C$, the **composition** $g \circ f : A \to C$ is defined as the function

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

for all $x \in A$.

Theorem 1.1.8 Properties of Compositions.

The composition of two (injections, surjections, bijections) is a(n) (injection, surjection, bijection).

Checkpoint 1.1.9 Prove Theorem 1.1.8.

Later in the course we will learn techniques for counting objects and proving that two sets have the same number of elements; the notion of cardinality will be a useful tool to remember.

Definition 1.1.10 Cardinality Relations.

Two sets A and B are said to have the **same cardinality**, written as

$$|A| = |B|,$$

if there exists a *bijection* between them.

We also say A has cardinality **less than or equal to** the cardinality of B, written as

$$|A| \leq |B|,$$

if there exists an *injective* function from A to B.

Checkpoint 1.1.11 There are as many natural numbers as odd integers. Prove that the set of odd integers

$$O = \{\ldots, -3, -1, 1, 3, \ldots\}$$

has the same cardinality as $\mathbb{N}$.

Hint. Construct a bijection from O to $\mathbb{N}$.

Definition 1.1.12 Power Set.

Let A be a set. The **power set** of A, denoted by $P(A)$, is the set

$$P(A) = \{X : X \subseteq A\},$$

that is, it contains all subsets of A.

Checkpoint 1.1.13 Prove that if A is finite, then

$$|P(A)| = 2^{|A|}.$$

1.2▲ Logic and Proof Techniques

Mathematical statements can typically be phrased as an implication $P \Rightarrow Q$, read as *if P, then Q*, where P or Q may be complex statements themselves that involve conjunctions (and), disjunctions (or), negations, quantifiers, even implications. There are various ways in which an implication can be proven true, and there is no hard and fast rule that dictates which proof method to use given a particular problem. In MAT102 you were introduced to the following proof techniques:

- Direct proof: Assume P is true, then prove Q is true.
- Contrapositive: Assume $\neg Q$ is true, then prove $\neg P$ is true.

- Contradiction: Assume the conclusion is false, then use this to arrive at a statement that contradicts one of the assumptions.

Activity 1.2.1

Prove each statement, noting which proof technique you used. Explain all your steps clearly, as if you are writing for the current batch of MAT102 students.

(a) The sum of two odd numbers is even.

(b) The square of an even number is divisible by 4.

(c) The equation $x^3 + x + 1 = 0$ has no rational solutions.

(d) For integer n, if $n^3 + 5$ is odd, then n is even.

(e) There is no smallest positive rational number.

(f) Every multiple of 4 can be written as $1 + (-1)^n(2n - 1)$ for some $n \in \mathbb{N}$.

(g) The sum of a rational number and an irrational number is irrational.

(h) A three-digit natural number is divisible by 9 if and only if the sum of its digits is divisible by 9.

(i) If A and B are defined as in Checkpoint 1.1.2, then $B \nsubseteq A$.

Many of these statements are *quantified* universally, which means it involves some variable (say n), and you need to prove the claim holds for all relevant values of the variable (say $n \in \mathbb{N}$). For 1, 2, and 4, for example, the relevant quantities are integers; the statements need to be proven for all integers.

We can use mathematical induction to prove that a statement is true for all natural numbers.

Theorem 1.2.1 Principle of Mathematical Induction.

Let $P(n)$ be a predicate defined for $n \in \mathbb{N}$. If the following conditions hold:

(a) $P(1)$ is true;

(b) For all $k \in \mathbb{N}$, $P(k) \Rightarrow P(k+1)$ is true.

then $P(n)$ is true for all $n \in \mathbb{N}$.

One can also replace the second condition with the following:
b. For all $k \in \mathbb{N}$, $[P(1) \wedge P(2) \wedge \cdots \wedge P(k)] \Rightarrow P(k+1)$ is true.*
*This is called **strong induction**, where one assumes the induction step holds for all natural numbers from 1 to k in order to prove the claim for $k + 1$.*

Depending on what is being proved, one may need to make slight modifications to the standard technique: e.g. changing/adding to the base case, or "skipping" from k to $k + 2$ in the case when one only has to prove the claim for every other natural number starting from the base case.

Checkpoint 1.2.2 Prove the following statements using induction:

(a) $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$ for all $n \in \mathbb{N}$.

(b) $2^n \geq n^2$ for all $n \in \mathbb{N}, n \geq 4$.

(c) $4^{2n} - 1$ is divisible by 5 for every $n \in \mathbb{N}$.

Checkpoint 1.2.3 The **Fibonacci sequence** $\{F_n\}$ is defined recursively as

$$\begin{cases} F_n = F_{n-1} + F_{n-2}, n \geq 3 \\ F_1 = F_2 = 1 \end{cases}.$$

Prove that

$$F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n$$

using strong induction.

Checkpoint 1.2.4 Let T_n be the number of ways one can tile a $2 \times n$ grid with 1×2 rectangles. For example, $T_2 = 2$ since there are two tilings of a 2×2 grid using only 1×2 rectangles.

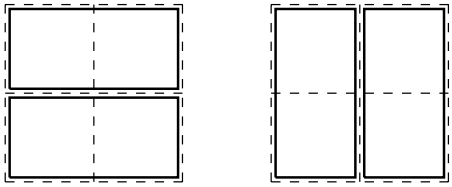


Figure 1.2.5 The two tilings of a two-by-two grid.

Find a recurrence relation for T_n and prove that $T_n = F_{n+1}$ as defined in Checkpoint 1.2.3.

1.3▲ Integers and Divisibility

For completeness we restate here the definition of divisibility and the Division Algorithm.

Definition 1.3.1 Divisibility and Primes.

Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus \{0\}$. We say that a **is divisible by** b, or b **divides** a, denoted by

$$b \mid a,$$

if there exists $m \in \mathbb{Z}$ such that $a = mb$.

If b is not divisible by a, then we write $b \nmid a$.

We say that the natural number p is a **prime number** if the only natural numbers that divide p are 1 and p.

Theorem 1.3.2 Division Algorithm.

Let $a, b \in \mathbb{N}$. Then there exist unique q and r that satisfy all of the following:

$$a = qb + r, q \geq 0, 0 \leq r < b.$$

Checkpoint 1.3.3 Find q and r that satisfy the Division Algorithm for the following pairs of numbers a and b:

(a) $a = 140, b = 22$

(b) $a = 22, b = 140$

(c) $a = 735, b = 21$

Definition 1.3.4 GCD.

Given integers a and b not both zero, their **greatest common divisor**, denoted by

$$\gcd(a, b),$$

is the largest integer that divides both numbers.

We say that a and b are **relatively prime** if $\gcd(a, b) = 1$.

There are a number of ways to determine the GCD of two numbers a and b:

- Listing all factors of a and b, then finding the largest one they have in common;
- Writing out the prime factorizations of a and b, then collecting all common prime factors;
- The Euclidean Algorithm (repeated division).

Checkpoint 1.3.5 Apply the three techniques above to compute $\gcd(220, 360)$.

Theorem 1.3.6 Bezout's Identity.

Let $a, b \in \mathbb{Z}$, not both zero. Then there exist $m, n \in \mathbb{Z}$ such that $am + bn = \gcd(a, b)$.

Checkpoint 1.3.7 Find a pair of integers x and y such that

$$13x + 11y = 2.$$

Then explain why the equation $13x + 11y = 2$ has infinitely many solutions. Can you characterize all such solutions?

Checkpoint 1.3.8 Prove that the equation

$$14x - 35y = 9$$

has no integer solutions.

Checkpoint 1.3.9 Let $a, b, d, \in \mathbb{N}$. Prove that $ax + by = d$ has integer solutions x and y if and only if $\gcd(a, b) \mid d$.

Lemma 1.3.10 Euclid's Lemma.

If p is prime, and a and b are integers such that $p \mid ab$, then either $p \mid a$ or $p \mid b$ (or both).

Checkpoint 1.3.11 Prove Lemma 1.3.10 using Theorem 1.3.6.

Checkpoint 1.3.12 Let $m, a, b \in \mathbb{N}$. Using Theorem 1.3.6, prove that if $m \mid ab$ and $\gcd(a, m) = 1$, then $m \mid b$.

1.4▲ Reading and Writing Proofs

Proofs are a form of communication. They are used to argue (that a claim holds true); and sometimes explain (*why* a claim is true).

Activity 1.4.1

When writing proofs, one needs to be *clear*, *complete*, and *correct*. Comment on the three proofs below of the statement

Let $m \in \mathbb{Z}$. Then m is even if and only if m^3 is even.

Which one(s) is/are

- convincing?
- easiest to read?
- missing steps?
- correct?

Proof 1 ($\Rightarrow$) $m = 2k \Rightarrow m^3 = 8k^3 = 2(4k^3)$, so m^3 is even.
($\Leftarrow$) By contradiction. Assume m^3 is even but m is odd. Then $m = 2k+1 \Rightarrow m^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1$, which is odd.
Contradiction, so m must be even. So m even $\Leftrightarrow$ m^3 even.
Proof 2

$$m \text{ even } \Leftrightarrow m = 2k \Leftrightarrow m^3 = 8k^3 \Leftrightarrow m^3 = 2(4k^3) \Leftrightarrow m^3 \text{ even},$$

hence proven.
Proof 3 We want to prove that

$$m \text{ is even if and only if } m^3 \text{ is even.}$$

($\Rightarrow$) First, we show m even $\Rightarrow$ m^3 even. If m is even, then we can write $m = 2k$ for some $k \in \mathbb{Z}$. Then,

$$\begin{aligned} m^3 &= (2k)^3 \\ &= 8k^3 \\ &= 2(4k^3). \end{aligned}$$

Since $k \in \mathbb{Z}$, then $4k^3 \in \mathbb{Z}$ as well, and so m^3 is even.
($\Leftarrow$) Next, we prove that m^3 even $\Rightarrow$ m even. To do this we prove the contrapositive: If m is odd, then m^3 is odd.
If m is odd, then there is a $k \in \mathbb{Z}$ such that $m = 2k + 1$. Then

$$\begin{aligned} m^3 &= (2k+1)^3 \\ &= 8k^3 + 12k^2 + 6k + 1 \\ &= 2(4k^3 + 6k^2 + 3k) + 1. \end{aligned}$$

Since $k \in \mathbb{Z}$, then $4k^3 + 6k^2 + 3k \in \mathbb{Z}$ as well. Therefore m^3 is odd. This completes the proof.

The use of English words makes proofs more approachable and understandable. Here are some commonly-used phrases in mathematical proofs. Note the use of the plural *we* instead of the singular *I*.

Declare intentions

- We will prove...
- We want to show that...
- In order to prove... we...
- At this point we need to find...
- We consider the following cases...

Clarify implications

- Since... then...
- Because..., we have...
- Therefore/thus/hence...
- This means that...
- The previous statement implies...

Explain steps

- By assumption, we know that...
- By simplication/manipulation,rearranging,...
- Because of property/theorem/definition, we have...

Activity 1.4.2

Write a complete and convincing proof of the following claim that uses the mathematical statements given below (in some order). Note that this is a proof by contradiction.

Claim: Let A, B be subsets of some universal set U. Prove that if $(A \cup B)^c = A^c \cup B^c$, then $A \subseteq B$.

$x \in A$	$x \in A^c \cup B^c$
$x \notin B$	$x \in A \cup B$
$x \in B^c$	$x \notin (A \cup B)^c$

Chapter 2

Counting Techniques

Short intro here

2.1 The Basic Counting Principles

Objectives

- State the Sum Rule and the Product Rule, and explain how the Product Rule derives from the Sum Rule.
- Given a counting problem, partition the objects being counted into subsets that facilitate the use of the Sum Rule.
- Given a counting problem, describe the steps necessary to form the object or scenario being counted, and apply the Product Rule.

In this section (and chapter) we will develop techniques for counting! When you hear the word *count* you probably think about *listing* or *enumerating* objects. For example:

- How many siblings do you have?
- Count the number of students enrolled in MAT202 this term.
- How many buildings are there on the UTM campus?

Often we are also interested in counting the number of different ways some given scenario or condition can happen. For instance, consider the following example:

Example 2.1.1 First Counting Example.

In the game *Kiss, Marry, Kill*,[1] you are given three different names, and you must decide which one among them to kiss/marry/kill (with the understanding that you can't kiss the person you marry, and the person you kiss, you can only kiss one time).

How many possible ways can you answer?

Solution. Suppose the three names are A, B, and C. We can just list all

possibilities to find that there are 6 ways:

Kiss	A	A	B	B	C	C
Marry	B	C	A	C	A	B
Kill	C	B	C	A	B	A

Example 2.1.1 is small enough that we can count the number of possibilities by listing them. Can you do the same for the following exercise? What do you notice about your answer to part (a)?

Checkpoint 2.1.2 Concert Seating. Three friends (Mina, Lisa, and Wendy) were able to get three seats together in a row at a Coldplay concert.

(a) How many ways can they choose to sit?

(b) How many ways can they sit if Lisa insists on sitting in the middle?

The techniques we will develop will help us count when the number of possibilities is too large that we can't simply list them all! For instance, the next example is one where listing all possibilities seems like a bad idea.

Example 2.1.3 Dog Adoption.

There are 10 dogs up for adoption at your local animal shelter. You and 9 other friends decide to adopt one dog each. How many ways can you assign dogs to people?

Solution (but not really) If we first fix you and your friends in some specified order (human 1, human 2, human 3, and so on) and name the dogs A, B, C, up to J, then each adoption arrangement corresponds to an *ordering of the letters A to J in a list*, where the position of each letter corresponds to the person adopting that dog.

For example, the arrangement

J	I	H	G	F	E	D	C	B	A
↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
1	2	3	4	5	6	7	8	9	10

means that dog J is assigned to human 1, dog I is assigned to human 2, and so on, while the arrangement DJABECIHGF means dog D is assigned to human 1, dog J to human 2, and so on...

You should quickly realize there are too many combinations to list!

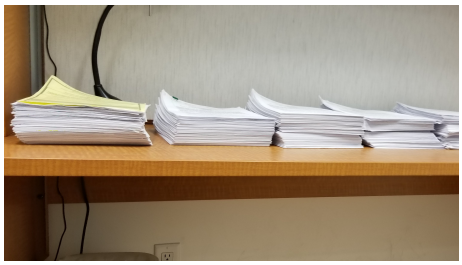
When possible, it is a good idea to *exploit the structure* of what we are counting! Two rules for counting will help us get started: the Sum Rule and the Product Rule. Think about the following checkpoint, which is similar to something you might have seen in grade school:

Checkpoint 2.1.4 Socks! You plan to move to a new apartment by the end of the month, and while packing your clothes, you note that you have 3 pairs of black socks, 4 pairs of white socks, and 2 pairs of blue socks.

How many pairs of socks do you have in total?

Checkpoint 2.1.5 Exam Counts. After an in-person term test or final exam, the course instructor and TAs get together and first verify that the number of papers handed in matches the number of students who wrote the test.

[1] You may know this game by a different name.



Can you think of an efficient way to count the papers?

Hint. You wouldn't just count them one by one...

In Checkpoint 2.1.4 the problem of counting the total number of pairs of socks had a straightforward solution. Since the socks were already separated by colour, and you knew how many of each colour you had, you just had to add the number of pairs for each colour to get the total.

For the test papers in Checkpoint 2.1.5 there are certainly multiple ways to do this. One method that TAs use is to form piles of ten, and count how many piles are produced. This is actually more similar to the socks example than you might think. Separating the huge pile of papers into groups of 10 has the same goal as separating socks by colour: one just has to add the numbers in each pile together in the end (which, if all piles have 10, is an easy calculation).

This is the **Sum Rule** in action.

Definition 2.1.6 Partition.

Let A be a finite set. We say that $B_1, B_2, \ldots, B_m$ form a **partition** of A if

- $B_i \cap B_j = \varnothing$ for all $i \neq j$, and
- $B_1 \cup B_2 \cup \cdots \cup B_m = A$.

Principle 2.1.7 Sum Rule.

If $B_1, B_2, \ldots, B_m$ form a partition of A, then

$$|A| = \sum_{i=1}^{n} |B_i| = |B_1| + |B_2| + \cdots + |B_m|.$$

The Sum Rule essentially tells us that in order to count a set of objects, we can break these objects up into disjoint cases, count each case separately, then add them all together in the end. Sounds reasonable!

Checkpoint 2.1.8 Twitter Followers. TJ is an avid Twitter user, where he manages the following accounts:

- A personal account with 200 followers;
- A K-pop stan Twitter account with 2500 followers;
- A third account with 12000 followers that tweets a picture of a puppy every hour.

Can you determine the total number of unique followers TJ has? Explain whether or not the Sum Rule is applicable to this problem.

Hint. To apply the Sum Rule, one needs to have a partition.

When we need to count objects that are constructed by performing *successive steps* or operations that are independent, we use the ***Product Rule***.

Principle 2.1.9 Product Rule.

If a certain operation takes k steps to accomplish, and if there are:

- *r_1 ways of performing step 1,*
- *r_2 ways of performing step 2 (regardless of how step 1 was performed),*
- *r_3 ways of performing step 3 (regardless of how step 2 was performed),*
- *and so on...*

Then, there are

$$\prod_{i=1}^{k} r_i = r_1 \cdot r_2 \cdot \ldots \cdot r_k$$

ways of performing steps 1 to k.

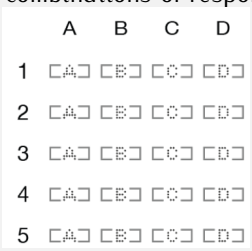
Checkpoint 2.1.10 Counting Outfits. You are deciding what outfit to wear to your Zoom class today. You have been putting off doing laundry, so you only have 3 clean shirts and 3 clean pairs of pants. Also, you have 8 pairs of socks to choose from. How many different outfits can you wear to school today? (Assume you cannot go to school shirtless, but you can go pantless or barefoot—no one will see!)

Checkpoint 2.1.11 Proof of the Product Rule. Use the Sum Rule to prove the Product Rule.

Hint. Induction on k.

Example 2.1.12 Multiple Choice Exam.

A multiple-choice exam has 20 questions and four choices for each question. How many possible combinations of responses are there?



Solution. Answering the whole test takes 20 individual, independent steps: picking one answer to each question. If we assume each question needs to have one answer, then in the statement of the Product Rule, $r_1 = 4$, $r_2 = 4$, and so on until $r_{20} = 4$, giving a total of

$$\underbrace{4 \times 4 \times \cdots \times 4}_{20 \text{ times}} = 4^{20} = 1099511627776$$

possible answer combinations.

In other words, pure guessing as a strategy will on average result in a perfect score once every one trillion tries. In comparison, the odds of matching six numbers in Lotto 6/49 is much better: one in 14 million.

If we allow questions to be left unanswered, then there are $5^{20} =$

95367431640625, around 96 trillion possible ways to answer the test.

Checkpoint 2.1.13 Concert Seating with n people. Apply the Product Rule to answer (a) and (b) of Checkpoint 2.1.2, then generalize this method to count the number of ways to sit n people in a row of n seats.

Because the following operation frequently turns up in counting problems, we have a special name for it.

Definition 2.1.14 Factorial.

For integer $n \geq 0$, the **factorial** of n, denoted by $n!$, is

$$n! = \prod_{i=1}^{n} i = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1.$$

By convention we define $0! = 1$.

Remark 2.1.15

For problems where the answer involves a factorial, it is fine to leave the factorial in your answer without computing the actual value.

Example 2.1.16 Dog Adoption, again.

Example 2.1.3 had too many combinations to list, but using the Product Rule we see that there are a total of

$$10! = 10 \times 9 \times 8 \times \cdots \times 1 = 3628800 \text{ combinations.}$$

Checkpoint 2.1.17 Trip Planning. Four friends (Andrew, Jagmeet, Yves-François, and Jo-Ann) are planning a trip to Ottawa, and they need to assign tasks (booking flights, booking hotel rooms, and making an itinerary) to three people. Andrew cannot be trusted to make an itinerary; also, either Jagmeet or Jo-Ann must book hotel rooms. How many ways can they assign tasks?

Think carefully about which counting principle(s) to apply here. Explain your method of calculation properly.

Hint. A diagram would be useful.

2.1.1 ▸▸ Solutions to Selected Checkpoints

Checkpoint 2.1.2 Concert Seating. Solution. a. Listing all possibilities yields 6 ways without any restrictions:

(Mina, Lisa, Wendy)	(Lisa, Wendy, Mina)	(Wendy, Mina, Lisa)
(Mina, Wendy, Lisa)	(Lisa, Mina, Wendy)	(Wendy, Lisa, Mina)

b. Exactly two of these seating arrangements has Lisa in the middle seat.

Checkpoint 2.1.4 Socks! Solution. It's not a trick question. $3 + 4 + 2 = 9$.

Checkpoint 2.1.8 Twitter Followers. Solution. If all followers among TJ's three accounts are different people, then we could just add

$$200 + 2500 + 12000 = 14700$$

to get the total number of unique followers. However this is very possibly not the case!

For instance, if we knew that a hundred of TJ's followers on his personal account also follow the puppy auto-tweeter, then the number of unique followers among all three accounts is no more than 14600. This is lower if there is more overlap.

The Sum Ruledoes not apply becase the three sets of followers do not form a partition of the set we want to count (the first condition fails).

Checkpoint 2.1.10 Counting Outfits. Solution. The operation of *picking an outfit to wear to school* can be broken down into the following steps:

1. Pick a shirt (3 choices)
2. Pick a pair of pants (4 choices, including no pants; regardless of which shirt you picked)
3. Pick a pair of socks (9 choices, including barefoot; regardless of which shirt/pants you wear)

So it takes 3 steps to decide on an outfit, where $r_1 = 3$, $r_2 = 4$, and $r_3 = 9$. By the Product Rule, there are $3 \cdot 4 \cdot 9 = 108$ different outfits you can choose to wear.

Checkpoint 2.1.13 Concert Seating with n people. Solution. We can generalize Checkpoint 2.1.2as follows: if n people want to sit in a row of n seats (with no restriction), then the whole operation of assigning seats to people takes n steps, where the first person has n seats to choose from, the next person has $n-1$, and so on, until 1 seat is left for the last person. The Product Rule then gives a total number of

$$n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1$$

ways that n people can sit in n seats in a row.

2.2▲ Permutations and Combinations

Objectives

- Derive the formulas for permutations and combinations (of n objects taken k at a time), multi-permutations, and permutations with repetitions allowed.
- Explain how overcounting is used as a counting technique and apply it to counting problems.
- Given a counting problem, recognize which of the above techniques is applicable, and use it to solve the problem.

In this section we get a little bit fancier and define some special quantities that show up frequently when counting objects or rearrangements. First, recall that the factorial of n is shorthand for the product

$$n! = n \times (n-1) \times \cdots \times 1,$$

which, as we saw in the previous section, can be used to count the number of ways to sit n people in a row for a concert.

Definition 2.2.1 Permutation.

A **permutation** is a bijection from a finite set S to itself.

Remark 2.2.2

If $|S| = n$, then there are $n!$ bijections $S \to S$. Equivalently,

- There are $n!$ ways to arrange n *distinct* objects in a row.
- There are $n!$ rearrangements of a word with n *distinct* letters. Each rearrangement is said to be a *permutation* of the n letters.

Example 2.2.3 Counting Bijections.

Let $S = \{a, b, c, d\}$. Then the function $f : S \to S$ defined by

$$f(a) = b, f(b) = d, f(c) = c, f(d) = a$$

is one example of a bijection from S to S. Since $|S| = 4$, there are a total of $4! = 24$ bijections from S to itself.

What if we wanted to rearrange k of the n distinct objects (i.e. only a subset)?

Checkpoint 2.2.4 EQUATION. How many four-letter words can be formed using the letters of the word

EQUATION?

Hint. How many choices do you have for the first letter? the second? the others? Use the Product Rule.

Let's generalize this. Let $k \leq n$, and use the Product Rule to count the number of ways to arrange k objects in a row, taking from a set of n distinct objects.

Then express your answer in terms of factorials, and complete the statement of Proposition 2.2.5 below.

Proposition 2.2.5 k-permutation of an n-set.

If $k \leq n$, then the number of permutations of k distinct elements from a set of size n, denoted by $P(n, k)$ or ${}_nP_k$, is

$$P(n, k) = \_\_\_\_\_ .$$

Remark 2.2.6

When solving problems you may use either notation above and leave your answer in that form.

Example 2.2.7 Student Council Representatives.

How many ways can a class of 45 students elect a president, vice-president, and secretary to represent them on student council?

Solution. This corresponds to the number of permutations of 45 objects taken 3 at a time, so the total is

$$45 \cdot 44 \cdot 43 = 85140.$$

One can also imagine the solution using the Product Rule: there are three steps to this operation:

elect a president:	45 choices
elect a vice-president:	44 choices
elect a secretary:	43 choices

Then the number of ways to do so is $45 \cdot 44 \cdot 43$.

Checkpoint 2.2.8 ZAHLEN.

(a) Count the number of three-letter words that can be formed from the letters of the word ZAHLEN.

(b) How many of the words from (a) contain ***only consonants***?

(c) How many of the words from (a) contain ***contain exactly one vowel***?

Hint. For part c., try using the Product Rule. What steps need to be performed to form a word that satisfies the given condition?

The next example shows that having *distinct* objects is crucial in the statement of Definition 2.2.1.

Example 2.2.9 Repeated Letters.

Count the number of arrangements of the letters in the word YEET.

Solution A misguided attempt to apply Definition 2.2.1 will yield $4! = 24$ possible arrangements of the word YEET. However, we see that there are only 12 possibilities when we list them all:

YEET	YETE	YTEE	TYEE	TEYE	TEEY
EETY	EEYT	ETYE	ETEY	EYET	EYTE

This is because the letters in the word YEET are *not* distinct! If we distinguish each letter E in the word by calling them E_1 and E_2, then we see that each arrangement above actually came from ***two*** arrangements, for instance:

$$YE_1E_2T \text{ and } YE_2E_1T \to YEET$$
$$YE_1TE_2 \text{ and } YE_2TE_1 \to YETE$$

Thus while Definition 2.2.1 predicts $4! = 24$ arrangements of the four letters Y, E_1, E_2, and T, we see that for each arrangement either E_1 is somewhere to the left, or somewhere to the right of E_2. Hence we divide by two to account for this overcounting, which gives the correct number, $4!/2 = 12$.

What if three letter E's are repeated? Following the same reasoning, we can distinguish them first as E_1, E_2, and E_3, then apply Definition 2.2.1. We will get a number that overcounts the actual answer by a factor of 6 this time, since there are $3! = 6$ ways to arrange the three E's:

$E_1E_2E_3$	$E_1E_3E_2$	$E_2E_1E_3$
$E_2E_3E_1$	$E_3E_1E_2$	$E_3E_2E_1$

We generalize this to Proposition 2.2.10, which gives a way to count rearrangements of words when some letters are repeated. (We say the letters are elements of a **multiset**, which generalizes sets to allow for multiple instances of elements.)

Proposition 2.2.10 Permutations of a multiset.

Let S be a set with n (not necessarily distinct) objects, such that there are n_1 objects of type 1, n_2 objects of type 2, ..., and n_k objects of type k, where $n_1 + n_2 + \cdots + n_k = n$. Then the number of arrangements of these objects is

$$\frac{n!}{n_1!n_2!\cdots n_k!}.$$

Checkpoint 2.2.11 MISSISSAUGA. How many arrangements can be formed using the letters of the word

MISSISSAUGA?

Checkpoint 2.2.12 MATHEMATICS. Count the number of ways the letters of the word MATHEMATICS can be arranged so that

(a) The two M's are beside each other.

(b) The two M's are *not* beside each other.

(c) The word MATH appears somewhere in the arrangement.

Hint 1. a. Treat 'MM' as a single object.

Hint 2. b. How are parts a. and b. related?

Hint 3. c. Treat 'MATH' as a single object.

Checkpoint 2.2.13 Esports Tournament. UTM Athletics is sending a team of 7 players to represent the university at an Ontario e-sports tournament called *The Provincial*. Suppose that a total of 30 students tried out for the team.

(a) How many possible teams can be formed from the students who tried out?

(b) Suppose further that there are different positions on the team, as follows

- 1 carry player
- 1 mid player
- 1 offlane player
- 2 support players
- 2 reserve players

How many possible teams can be formed from the students who tried out? Assume everyone who tried out can play every position. (Not usually the case in reality...)

Hint 1. a. Each student either makes the team, or doesn't. Express each possible team as a sequence of 30 labels, one for each student who tried out.

Hint 2. b. Same with a., but with more labels to account for the different positions on the team.

The scenario in part (a) of Checkpoint 2.2.13 is an example where the order in which the students are picked does not matter -- the team is just a collection (set) of 7 players. Here's a smaller example:

Example 2.2.14 Picking Bridesmaids.

Adele is getting married soon, and due to space constraints at the venue, needs to pick exactly two of her five best friends (Mel B., Mel C., Emma,

Geri, and Victoria) to be her bridesmaids. How many possible combinations are there?

Solution Each combination of bridesmaids corresponds to a rearrangement of three X's and two O's, given a *fixed* arrangement of the five names in a row; for instance, the arrangement

Mel B.	Mel C.	Emma	Gerri	Victoria
O	X	X	O	X

means that Mel B. and Gerri will be bridesmaids, while

Mel B.	Mel C.	Emma	Gerri	Victoria
X	X	X	O	O

corresponds to Geri and Victoria being chosen. Applying Proposition 2.2.10 to the three X's and two O's, we see that there are exactly $\frac{5!}{2!3!} = 10$ possible combinations.

Note When the usual formula for k-permutations from an n-set (Proposition 2.2.5)) is applied to the previous example, we get a total of $\frac{5!}{(5-3)!} = 60$, which is incorrect. The reason is that this formula treats the pairs

(Geri, Victoria) and (Victoria, Geri)

as different outcomes, while for this example they both correspond to the same combination of {Geri, Victoria} being chosen as bridesmaids, since the order doesn't matter.

Overcounting as a Counting Technique.

In the previous examples you may have been reminded of the main difference between an *n-tuple* $(a_1, a_2, \ldots, a_n)$ and a *set of n elements* $\{a_1, a_2, \ldots, a_n\}$: order.

To give a small example, the triples $(1, 2, 3)$ and $(3, 1, 2)$ are *not* equal in $\mathbb{R}^3$, and there are a total of six *different* triples using these same numbers:

$(1, 2, 3)$	$(2, 1, 3)$	$(3, 1, 2)$
$(1, 3, 2)$	$(2, 3, 1)$	$(3, 2, 1)$

On the other hand, the sets $\{1, 2, 3\}$ and $\{3, 2, 1\}$ are equal—it doesn't matter how we write the three numbers since a set is defined by object membership.

In general, to count objects for which order does not matter, we can ***assume order matters first, then divide by the overcounting factor***, typically the factorial of how many elements are under consideration.

As another example, in Proposition 2.2.10, each $n_i!$ term in the denominator is the overcounting factor associated with first treating all objects of type i (there are n_i of them) differently.

When selecting k elements from a set of n, and if the order in which they are selected does not matter, we simply need to divide by $k!$.

Definition 2.2.15 Combination.

A **combination** of k elements taken from a set S of size n is any k-element subset of S.

Proposition 2.2.16 k-combinations of an n-set.

The number of k-combinations of a set with n distinct elements, denoted by $\binom{n}{k}$ (read as 'n choose k'), is

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

Alternative notation for this include $C(n,k)$ and ${}_nC_k$.

Example 2.2.17 Counting Cards.

A **standard deck of cards** consists of 52 cards, which come in 13 ranks (A/ace, 2, 3, 4, 5, 6, 7, 8, 9, 10, J/jack, Q/queen, K/king) of four cards each, one for each suit: clubs ♣ (a black suit), spades ♠ (black), hearts ♡ (red), diamonds ♢ (red).

(a) How many outcomes (or ***hands***) are possible when you draw five cards at random from the deck?

(b) How many of these five-card hands comprise only numbered cards?

(c) How many of these five-card hands have exactly two red and three black cards?

Solution a. There are 52 distinct cards in the deck, and we are drawing five of them at random. Each outcome only depends on which cards are drawn, so the order in which we draw them does not matter. Therefore there are

$$\binom{52}{5} = \frac{52!}{47!\ 5!} = 2598960$$

possible five-card hands.

b. The ranks 2 to 10 are the numbered cards; there are a total of 36 numbered cards in a deck (9 ranks times 4 suits each). The number of five-card hands drawn from these cards is

$$\binom{36}{5}.$$

c. The process of forming such a five-card hand can be broken down into two steps:

Step 1: Pick two red cards

Step 2: Pick three black cards

These two steps are independent of one another. There are 26 black and 26 red cards, so the Product Rule tells us that there are

$$\binom{26}{2}\binom{26}{3}$$

five-card hands with this property.

Checkpoint 2.2.18 Esports Tournament, again. Solve part a. of Checkpoint 2.2.13 using Proposition 2.2.16

Then solve part b. (and express your answer) using only combinations.

Checkpoint 2.2.19 Two Ways of Counting. Let $0 \leq k \leq n$. Using algebra it's straightforward to show that

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

Without using algebra, explain why $\binom{n}{k}$ is equal to $\binom{n}{n-k}$ by counting the number of k-subsets of $\{1, 2, \ldots, n\}$ in two ways.

Hint. The first way is the usual way. For the second way: select elements that will *not* be put in the k-set.

Exploration 2.2.1 Early Combinatorics.

Some of the earliest mentions of permutations and combinations occur in ancient Hindu texts dating back to the year 600 BC. Called *vikalpa* and *bhaga*, respectively, they were used in the study of Vedic meters in poetry, in architecture, in medicine, astrology, and other areas.

The following examples are taken from [5].

(a) The *Suśruta-sahitā*, (est. 500 BC) an ancient Hindu text on medicine and surgery, counts the number of combinations of the flavours *sweet*, *acid*, *saline*, *pungent*, *bitter*, and *astringent* taken two at a time, in the following way:

> "On making two combinations in successive way, those beginning with sweet are found to be 5 in number; those beginning with acid are 4; those with saline 3; those with pungent 2; bitter and astringent make 1 combination."
>
> —*Suśruta-sahitā* lxiii, as cited in [5], p. 358

Explain how this computes $\binom{6}{2}$.

(b) This excerpt from the *Anuyogadvāra-sūtra* (c. 500) explains how to compute 6!.

> "What is the direct arrangement? Dharmāstikāya, Adharmāstikāya, Ākāśāstikāya, Jīvāstikāya, Pudgalāstikāya and Addhāsamaya—this is the direct arrangement. What is the reverse arrangement? Addhāsamaya, Pudgalāstikāya, Jīvāstikāya, Ākāśāstikāya, Adharmāstikāya, and Dharmāstikāya—this is the reverse arrangement. What are the mixed arrangements? From the series of numbers beginning with one and increasing by one up to six terms. The mutual products of these minus 2 will give the number of mixed arrangements."
>
> —*Anuyogadvāra-sūtra*, Sūtra 97, as cited in [5], p. 363.

Discuss what *mixed arrangement* refers to and how the computation of 6! is carried out.

2.2.1 ▸▸ Solutions to Selected Checkpoints

Checkpoint 2.2.8 **ZAHLEN. Solution.** c. First, pick two consonants out of the four: ${}_4P_2$ two-letter words can be formed. Then, pick a vowel (2 choices), and insert it into the two-letter word (3 possible slots) to form the required three-letter word with exactly one vowel. Thus the total number of such words is

$$ {}_4P_2 \times 2 \times 3 = 72. $$

Checkpoint 2.2.12 **MATHEMATICS. Solution.** c. Treating 'MATH' as a single object, we reduce the problem to counting the number of arrangements of eight distinct objects:

'MATH' E M A T I C S

Hence there are 8! rearrangements of MATHEMATICS where the word MATH appears.

Checkpoint 2.2.18 **Esports Tournament, again. Solution.** First, we select the carry player: there are $\binom{30}{1}$ ways to do so.

Then we can select the mid player in $\binom{29}{1}$ ways regardless of who was picked to be carry. (Pick one player out of the 29 remaining.)

The offlane player can be picked in $\binom{28}{1}$ ways.

To pick supports, $\binom{27}{2}$ possible combinations. Selecting reserve players, $\binom{25}{2}$ choices.

Hence there are

$$ \binom{30}{1}\binom{29}{1}\binom{28}{1}\binom{27}{2}\binom{25}{2} $$

possible team combinations.

2.3▲ Binomial Coefficients

Objectives

- Prove the Binomial Theorem and apply it to find coefficients of terms in expansions.
- Describe and prove simple identities involving binomial coefficients possibly in relation to Pascal's Triangle.

In this section we discuss the quantity $\binom{n}{k}$ in more detail and explore some nice related identities and applications. First, we give a name to the quantity; the reason for the name will be made clear in the main theorem of this section.

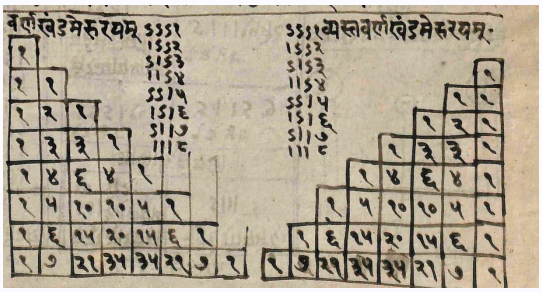
Definition 2.3.1 Binomial Coefficient.

For $k \leq n$, the quantities

$$ \binom{n}{k} $$

are called **binomial coefficients**.

Exploration 2.3.1 The Meru Prastaara (The Holy Mountain).



The Indian mathematician and writer Pigala (200 BC) in his text the *Chandaśāstra* studied variations in poetic metres when using only either long (*g*, for *guru*) and short (*l*, for *laghu*) syllables.

This exposition is based on [5], p. 390.

He explained that monosyllabic (or one-syllable) metres have two variations—either *g* or *l*—while disyllabic metres have four different kinds:

gg, *gl*, *lg*, or *ll*.

Or, one with no *l*'s, two with one *l*, and one with two *l*'s.

Pigala also observed that each two-syllable variant could be obtained from the one-syllable variants using the following scheme, appending on the right:

monosyllabic	*(g*	*l)*	*(g*	*l)*
append	*g*		*l*	
disyllabic	*gg*	*lg*	*gl*	*ll*

The same can be done going from two to three syllables.

disyllabic	*(gg*	*lg*	*gl*	*ll)*	*(gg*	*lg*	*gl*	*ll)*
append	*g*				*l*			
trisyllabic	*ggg*	*lgg*	*glg*	*llg*	*ggl*	*lgl*	*gll*	*lll*

(a) Of the three trisyllabic variants with two *l*'s (*llg*, *lgl*, and *gll*), one comes from the first group (ending with *g*), and two from the second (ending with *l*). Explain how this demonstrates that

$$\binom{3}{2} = \binom{2}{2} + \binom{2}{1}.$$

(b) Construct the table for the four-syllable forms in a similar way: appending *g*'s to all trisyllabic forms, then appending *l*'s. You should get a total of 16. In the same manner as (a), find an identity involving

$$\binom{4}{2}$$

by looking at the two possible endings of the four-syllable forms.

Hint. There are six strings involving *g*'s and *l*'s that have exactly two *l*'s. How many of them end with *g*? How many with *l*?

(c) Generalize the arguments above to a formula involving

$$\binom{n}{k}.$$

Hint 1. Separate into two cases depending on the last syllable (*g* or *l*).

Hint 2. How many of the $(n-1)$-syllable variants already have k *l*'s? How many have $(k-1)$ *l*'s and need one more?

Answer. Right-hand side is $\binom{n-1}{k} + \binom{n-1}{k-1}$.

In Exploration 2.3.1 we saw how the binomial coefficient $\binom{n}{k}$ can be expressed as the *sum* of two binomial coefficients involving $(n-1)$:

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

This rule is known as Pascal's Formula, after mathematician Blaise Pascal, who formalized many of the results and identities about the binomial coefficients.

Theorem 2.3.2 Pascal's Formula.

If $n \geq 1$, then

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

Theorem 2.3.2 generates an intuitive visualization of the binomial coefficients that you may have seen before, widely known as Pascal's Triangle.

Pascal was not the first to discover this mathematical object, which was simply called the **arithmetical triangle** beforehand.

This triangle and its relations to combinatorial problems was known to several other mathematicians: Pigala, and several others in India; Chinese mathematicians Jia Xian and Yang Hui; Ahmad Ibn Mun'im, who taught in Marrakesh; Niccolò Tartaglia and Gerolamo Cardano (Italy); Michael Stifel (Germany); and Marin Mersenne, who met and did mathematics with Pascal.

For more details check out [6] for an excellent resource.

We start by placing a 1 in the 0th row, and two 1's in the 1st row. Then each new row starts and ends with a 1, while each value in between is obtained by adding the numbers to its upper left and upper right.

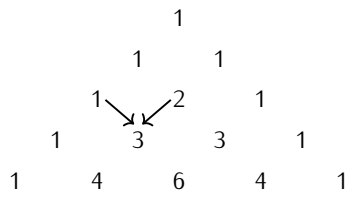


Figure 2.3.3 The first five rows of Pascal's Triangle, for $n = 0$ to 4.

The kth entry in the nth row of this triangle (starting with $n = 0$) is exactly $\binom{n}{k}$, while Theorem 2.3.2 shows how to recursively generate its rows.

Checkpoint 2.3.4 Continue the Triangle. Complete Pascal's Triangle up to the 9th row and use it to determine the value of $\binom{9}{3}$.

The reason for the term *binomial coefficient* is clarified in the next theorem.

Theorem 2.3.5 Binomial Theorem.

For $k \leq n$, the quantity $\binom{n}{k}$ is equal to the coefficient of $x^{n-k}y^k$ in the expansion of $(x+y)^n$. That is,

$$(x+y)^n = \underbrace{(x+y)(x+y)\cdots(x+y)}_{n \text{ times}} = \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k.$$

Proof. Each factor in the product $(x+y)^n = (x+y)(x+y)\cdots(x+y)$ contributes either an x or a y in the resulting expansion. We can express each term in the answer as a sequence of n symbols, each either an x or a y; for example, picking x from each $(x+y)$ term gives $\underbrace{xx\cdots x}_{n \text{ times}} = x^n$.

Hence the number of times $x^{n-k}y^k$ appears in the final expansion is precisely the number of rearrangements of the word

$$\underbrace{x\ x\cdots x}_{n-k \text{ times}}\underbrace{y\ y\cdots y}_{k \text{ times}},$$

which is exactly equal to $\frac{n!}{(n-k)!k!} = \binom{n}{k}$ by Proposition 2.2.10.

Observe that the proof of Theorem 2.3.5 simply counts the number of n-letter strings of x's and y's that contain k number of x's. This is the same thing as counting n-syllable forms in Exploration 2.3.1, and in fact, Theorem 2.3.5 can also be proven using the same recursive argument in Exploration 2.3.1 part (c).

Checkpoint 2.3.6 Coefficient of x^4y^7 in $(x+y)^{11}$. Determine the coefficient of x^4y^7 in the product $(x+y)^{11}$.

Checkpoint 2.3.7 Coefficient of a^2b^3. Determine the coefficient of a^2b^3 in each product:

(a) $(a+b)^5$

(b) $(a-b)^5$

(c) $(3a+2b)^5$

Hint. b. and c. What are x and y in the statement of Theorem 2.3.5?

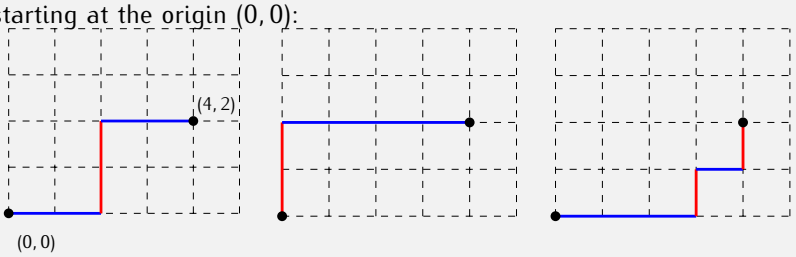
Checkpoint 2.3.8 Prove that $\sum_{k=0}^{n} \binom{n}{k} = 2^n$. Prove that $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ for $n \geq 0$.

Hint. Stare at Theorem 2.3.5 until you see it.

We end this section with a nice application where binomial coefficients appear.

Example 2.3.9 Lattice Paths.

On the xy-plane, a **lattice path** is a path that moves from integer point to integer point by taking only steps of length one to the right or upwards. For instance, the following are three different paths to the point $(4, 2)$, starting at the origin $(0, 0)$:



Each path above can be represented as a sequence of 4 R's and 2 U's:

RRUURR UURRRR RRRURU

so the total number of lattice paths from $(0, 0)$ to $(4, 2)$ is the same as the number of such sequences, which is

$$\binom{6}{4} = \frac{6!}{2!\ 4!}.$$

Example 2.3.9 illustrates a useful technique in counting problems: by representing what is being counted (lattice paths) in a different way (sequences of R's and U's), we can uncover the combinatorial structure of these objects, making them easier to count.

Checkpoint 2.3.10 Lattice Paths to (a, b). Count the number of lattice paths ending at (a, b) for integer $a, b \geq 0$.

Checkpoint 2.3.11 Lattice Paths, specific numbers. Determine the number of lattice paths that end at:

(a) $(5, 4)$

(b) $(4, 4)$

(c) $(5, 3)$

Simplify your answers to arrive at a single number for each part. How are your answers related?

Checkpoint 2.3.12 Lattice Paths and Pascal's Formula. Prove Theorem 2.3.2 using lattice paths and an idea from Checkpoint 2.3.11.

Hint. Count the number of lattice paths to $(k, n - k)$.

2.3.1 ▸▸ Solutions to Selected Checkpoints

Checkpoint 2.3.7 Coefficient of a^2b^3. Solution. b. Take $x = a$ and $y = -b$ with $n = 5$ in Theorem 2.3.5. The term a^2b^3 corresponds to the index $k = 3$, which is

$$\binom{5}{3} a^{5-3}(-b)^3 = -\binom{5}{3} a^2b^3,$$

and so its coefficient is $-\binom{5}{3} = -10$.

Checkpoint 2.3.8 **Prove that** $\sum_{k=0}^{n} \binom{n}{k} = 2^n$. **Solution**. The result follows from substituting $x = 1$ and $y = 1$ into the statement of Theorem 2.3.5.

Checkpoint 2.3.10 **Lattice Paths to** (a, b). **Solution**. The number of lattice paths to the point (a, b) is the same as the number of strings of length $a + b$ with a R's and b U's, and this is equal to

$$\frac{(a+b)!}{a!\ b!} = \binom{a+b}{a} = \binom{a+b}{b}$$

by Proposition 2.2.10.

Checkpoint 2.3.12 **Lattice Paths and Pascal's Formula. Solution**. Any lattice path from $(0, 0)$ to the point $(k, n-k)$ either passes through the point $(k-1, n-k)$ (and takes one last step to the Right) or the point $(k, n-k-1)$ (and takes one last step Upwards). This is a partition of the set of lattice paths to $(k, n-k)$. We also know from Checkpoint 2.3.10 that there are $\binom{n}{k}$ lattice paths to $(k, n-k)$.

Furthermore, by Checkpoint 2.3.10 there are $\binom{n-1}{k-1}$ lattice paths to $(k-1, n-k)$ and there are $\binom{n-1}{k}$ lattice paths to $(k, n-k-1)$.

Hence by Principle 2.1.7, we must have

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

as desired.

2.4▲ The Balls in Bins Formula

Objectives

- Derive the formulas for permutations and combinations with repetition (Balls in Bins Formula).
- Given a counting problem, recognize which of the above techniques is applicable, and use it to solve the problem.

Consider the following example similar to Example 2.1.12.

Example 2.4.1 Multiple Choice, again.

A standardized multiple-choice test for high school students has 40 questions and 5 choices each (A to E). How many possible ways can the test be answered?

Solution. For each question, there are 5 options, so using Principle 2.1.9, there are a total of 5^{40} possible ways to complete the test.

The operation in Example 2.4.1 is called a permutation where *repetition* or *replacement is allowed*, since

- The order in which the answers are picked matters (i.e. A-B-A is different from B-A-A); and
- Answers can be repeated. Imagine a bag with five balls labeled A to E; for each question we draw a ball from the bag, record the answer, and put it back.

We formalize this in the next result.

Proposition 2.4.2 Permutations with repetition.

If repetition is allowed, the number of permutations of k objects taken from a set of size n is n^k.

Proof. By Principle 2.1.9, since there are n possibilities for each of the k choices, the total number of ways to do so is n^k.

There is also a counterpart for combinations in which the order does not matter, which the next example illustrates.

Example 2.4.3 Rice Advice.

Ten participants are recruited to join a focus group discussion on rice, after which they are asked to indicate their preferred type of rice among the following options:

- Arborio
- Basmati
- Jasmine
- Koshihikari
- Malagkit

The participants gave their preferences anonymously so the researchers only know how many participants responded with each option. How many combinations of answers can the researchers obtain from the study?

Solution Since we are only concerned with the survey results, outcomes look like the following, where we only record how many respondents picked the corresponding option:

Arborio -- 3, Basmati -- 5, Jasmine -- 2

and

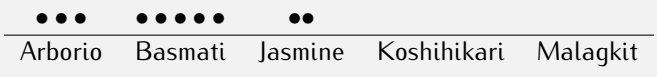
Koshihikari -- 9, Malagkit -- 1

are examples of possible outcomes; we need to count how many there are in total.

Note that we cannot simply take permutations and then divide by an overcounting factor since how much we overcount by depends on the actual distribution of answers.

Instead, we envision the process of collecting survey responses as placing balls into bins with labels `Arborio,' `Basmati,' and so on. (Imagine the participants physically placing their survey forms into one of five ballot boxes!)

For example, the outcome [Arborio -- 3, Basmati -- 5, Jasmine -- 2] corresponds to the following distribution of balls into bins:



This can also be represented concisely as the pattern

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

where the four vertical lines denote 'dividers' in between each pair of adjacent bins. Hence the problem of counting the number of possible outcomes is reduced to counting the number of arrangements of 10 $\bullet$ and 4 $|$ symbols, which is

$$\frac{14!}{10!\,4!} = \binom{14}{4}$$

by Proposition 2.2.10.

Checkpoint 2.4.4 Rice Advice Exercise. Following Example 2.4.3, express each survey outcome as a pattern of dots $\bullet$ and bars $|$, or vice-versa.

(a) Jasmine -- 3, Basmati -- 3, Arborio -- 1, Malagkit -- 3

(b) Koshihikari -- 10

(c) $\bullet\bullet\,||\,\bullet\bullet\bullet\bullet\bullet\bullet\,||\,\bullet\bullet$

(d) $||\,\bullet\bullet\bullet\bullet\bullet\,|\,\bullet\,|\,\bullet\bullet\bullet\bullet$

Hint. Make sure the bins are in the right order!

This is called a *combination where repetition is allowed*, since

- The order in which objects are picked *does not matter* (i.e.~A-B-A is the same as B-A-A); and
- Objects can be repeated.

As we saw in Example 2.4.3, the number of k-combinations taken from a set of size n when repetition is allowed is equal to the number of ways we can distribute k balls into n bins. This gives the following formula:

Theorem 2.4.5 Balls in Bins.

If repetition is allowed, the number of combinations of k objects taken from a set of size n is

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

This is also equal to the number of ways one can distribute k indistinguishable balls into n bins.

Proof. The total number of these combinations is equal to the number of ways to arrange k bullets ($\bullet$ symbols; one for each object), and $n-1$ bars ($|$ symbols; to delineate bins):

$$\underbrace{\bullet\ \bullet\ \cdots\ \bullet}_{k \text{ copies}}\ \underbrace{|\ |\ \cdots\ |}_{n-1 \text{ copies}},$$

which is $\binom{k+n-1}{k}$ or $\binom{k+n-1}{n-1}$ by Proposition 2.2.10.

Remark 2.4.6 Stars and Bars.

Some textbooks refer to Theorem 2.4.5 as the *Stars and Bars Formula*, replacing the bullet symbols with stars, i.e.

$$\underbrace{\star\ \star\ \cdots\ \star}_{k \text{ copies}}\ \underbrace{|\ |\ \cdots\ |}_{n-1 \text{ copies}}.$$

Checkpoint 2.4.7 Apples to Students. A teacher has 20 apples that are to be handed out to 9 students.

(a) How many different ways are there of distributing the apples?

(b) How many different ways are there of distributing the apples so that *each student receives at least one apple*?

Hint. b. Give one apple to each student to begin, then distribute the rest.

A nice application of the Balls in Bins Formula is counting the number of nonnegative integer solutions to equations of the form

$$x_1 + x_2 + \cdots + x_n = k.$$

Exploration 2.4.1 Nonnegative integer solutions.

Consider the following equation:

$$x_1 + x_2 + \cdots + x_5 = 10, \tag{2.4.1}$$

and suppose we're interested in its nonnegative integer solutions.

(a) Verify that $(x_1, x_2, x_3, x_4, x_5) = (3, 5, 2, 0, 0)$ is a nonnegative integer solution to (2.4.1). Then explain how we can view this solution as an assignment of balls into labeled bins.

(b) Using Theorem 2.4.5, count the number of nonnegative integer solutions to (2.4.1).

(c) Generalize the above argument to count the number of nonnegative integer solutions to

$$x_1 + x_2 + \cdots + x_n = k.$$

State explicitly what the balls and the bins are.

Proposition 2.4.8 Nonnegative integer solutions.

The number of nonnegative integer solutions to $x_1 + x_2 + \cdots + x_n = k$ *is*

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

Checkpoint 2.4.9 Determine the number of integer solutions to the system

$$\begin{cases} x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 15 \\ x_1, x_2, x_3, x_4, x_5, x_6 \geq 0 \end{cases}$$

Checkpoint 2.4.10 Nonnegative integer solutions with additional constraints. Determine the number of integer solutions to the equation

$$x_1 + x_2 + x_3 + x_4 = 77$$

such that:

(a) x_1, x_2, x_3, x_4 are nonnegative.

(b) $x_1 \geq 4$, $x_2 \geq 0$, $x_3 \geq 12$, and $x_4 \geq 9$.

(c) $0 \leq x_1 \leq 30$, and $x_2, x_3, x_4 \geq 0$.

Hint 1. b. Look at part (b) of Checkpoint 2.4.7.

Hint 2. c. Solve the problem with $x_1 \geq 31$ first then subtract from part (a).

2.4.1 ▸▸ Solutions to Selected Checkpoints

Checkpoint 2.4.10 Nonnegative integer solutions with additional constraints. Solution. b. In the context of Checkpoint 2.4.7, $x_1 \geq 4$ means that the first student must get at least 4 apples, so we start off by giving 4 to the variable x_1. We can model this by defining a new variable

$$y_1 = x_1 - 4,$$

where y_1 represents *how many more apples* above 4 we assign to x_1.

We can rearrange to get $x_1 = y_1 + 4$ and substitute this into the original equation to get the new system

$$\begin{cases} y_1 + x_2 + x_3 + x_4 = 73 \\ y_1 \geq 0, x_2 \geq 0, x_3 \geq 12, x_4 \geq 9 \end{cases}$$

Then the same process can be repeated for x_3 and x_4, resulting in the system

$$\begin{cases} y_1 + x_2 + y_3 + y_4 = 52 \\ y_1 \geq 0, x_2 \geq 0, y_3 \geq 0, y_4 \geq 0 \end{cases}.$$

At this point it is the same kind of system as in Proposition 2.4.8, hence we can apply it directly to get the desired number, $\binom{56}{53}$.

2.5▲ Combinatorial Arguments

Objectives

- Prove simple combinatorial identities by counting a set in two ways. (The set may or may not be given.)

The Binomial Theorem and Pascal's Formula are examples of **combinatorial identities**. These are identities or equations that involve the binomial coefficients.

We've seen two possible proofs of Pascal's Formula

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

in Exploration 2.3.1 and Checkpoint 2.3.12. One can prove this a third way using algebra.

Checkpoint 2.5.1 Pascal's Formula, again. Prove Theorem 2.3.2 by manipulating the right-hand side algebraically, and showing that it simplifies to the left-hand side.

Proofs by algebra are easy to follow, but often provide little information about *why* the statement is true. The first two proofs of Theorem 2.3.2, in contrast, provide insights about the quantities involved in the identity. Let's look at another example.

Theorem 2.5.2 Chairperson Identity.

For integers $0 \leq k \leq n$,

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

Checkpoint 2.5.3 Chairperson by Algebra. Prove Theorem 2.5.2 using algebra.

Now we prove Theorem 2.5.2 a second way, with what we call a **combinatorial argument** or a **combinatorial proof**. This typically involves counting one set in two different ways, thus showing that the two quantities obtained (from each way of counting) are equal.

Example 2.5.4 Chairperson by Combinatorial Proof.

Prove Theorem 2.5.2 by counting a set in two ways.

Solution. Our goal is to show that

$$k\binom{n}{k} = n\binom{n-1}{k-1} \tag{2.5.1}$$

given integers $0 \leq k \leq n$.

To do this, we count the number of ways to form a committee of k members from n people, and then elect a chair of the committee.

Suppose that from a group of n people, we want to

1. Form a committee of k people; and
2. Elect a chair of the committee.

By Principle 2.1.9, we can count the number of ways we can do this by multiplying.

1. There are $\binom{n}{k}$ ways to form a committee of k people from a group of n.
2. From the k people in the committee, we need to choose a chair, and there are k choices.

Hence we count a total of

$$\binom{n}{k} \times k$$

ways to do this. Note that this is the left-hand side of what we're proving, (2.5.1).

Now let's count the number of such committee-chair selections in a different way: by first selecting the chair.

1. Elect a chair of the committee; then
2. Complete the committee by adding members.

Again, we use Principle 2.1.9, noting that the number of choices in the second step is independent of who is picked for the first.

1. There are n people in the original group, so we have n choices for committee chair.
2. From the remaining $n-1$ people, we need to select $k-1$ members to fill out the committee. There are $\binom{n-1}{k-1}$ ways to do this.

Therefore we can select a chair and form the committee a total of

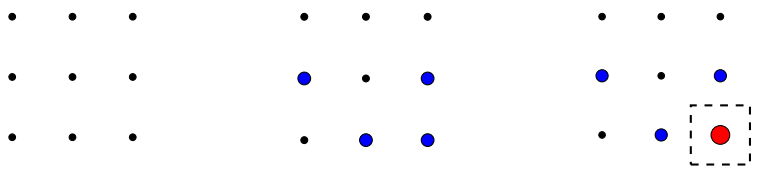
$$n\binom{n-1}{k-1}$$

ways. This is the right-hand side of (2.5.1)!

We just showed that the left-hand side and the right-hand side of the given identity are two different ways of counting the committee-chair possibilities, and hence, they must be equal.

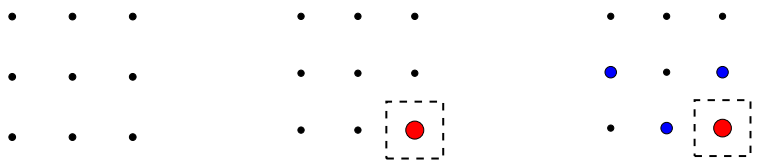
The following diagrams illustrate the two ways of selecting a committee of size $k = 4$ and a chairperson given a group of $n = 9$ people.

First way of counting:



From nine people | pick four members | then elect a chair.

Second way:



From nine people | elect a chair | then pick three more members.

While the combinatorial proof of the Chairperson Identity is no more correct than the algebraic method, it offers a concrete, meaningful way to explain why the two quantities are always equal. Proving combinatorial identities in this manner requires creativity, especially if one is not told *what set* is being counted.

In general:

- If the identity involves addition, this means the objects being counted will likely be broken up into disjoint cases (and Principle 2.1.7 is used).
- If the identity involves multiplication, there may be multiple interpretations depending on the use of Principle 2.1.9. For instance, 2^n may represent the number of subsets of $\{1, 2, \ldots, n\}$ or the number of binary strings of length n.

Checkpoint 2.5.5 **Prove** $n^2 = 2\binom{n}{2} + n$**.** Using algebra it is a straightforward manipulation to show that

$$n^2 = 2\binom{n}{2} + n$$

for $n \in \mathbb{N}$. Write a complete combinatorial proof of this statement.

Hint. First think what objects are counted by n^2. Then, break them up into two distinct cases for the right-hand side

Checkpoint 2.5.6 **Another proof of Checkpoint 2.3.8.** Prove the statement in Checkpoint 2.3.8 by counting the number of subsets of $\{1, 2, \ldots, n\}$ in two ways.

Hint. Partition subsets by cardinality.

2.6 Summary

In this chapter we developed techniques applicable to a wide variety of counting problems. One should be able to decide which technique to use by determining if order matters or not; if repetition is allowed or not; if the underlying set is a multi-set or not. Table 2.6.1 summarizes these considerations.

Keep in mind that the Sum Rule and Product Rule underpin all these formulas, and that there is often more than one solution to any given counting problem.

Table 2.6.1 Summary of Counting Techniques

	Permutation (order matters)	Combination (order does not matter)
no repetition	Proposition 2.2.5	Proposition 2.2.16
with repetition	Proposition 2.4.2	Theorem 2.4.5
multiset	Proposition 2.2.10	– – – – –

2.7 Exercises

Additional Exercises for Chapter 2

1. The latest album release from the worldwide famous Kpop group *ONCE* has four different versions for sale: versions L, O, V, and E. Preorder numbers by version as reported by Korean newspaper *Dispatched* are as follows:
   - L: 20,000
   - O: 25,000
   - V: 22,500
   - E: 30,000

   How many units did *ONCE*'s album move in preorders, total? Can we also determine how many *people* preordered the album?
2. The local bank *Factorial Financials* enforces the following restrictions on its online banking passwords:
   - Should only contain alphanumeric characters (A-Z, 0-9);
   - Should be exactly 8 characters in length; and

- Should start and end with a letter.

How many possible passwords can be created?

3. A new format for passenger vehicle licence plates issued in the province is being proposed, that adheres to the following conditions:
   - Pattern is AB123-4CD (or letter-letter-digit-digit-digit--digit-letter-letter).
   - The letters G, I, O, Q and U cannot be used.
   - The first digit cannot be a zero.
   - The last two letters must be different.

   How many licence plates combinations are possible that satisfy all these conditions?
4. How many arrangements of the word PANINI
   (a) end with the letter P?
   (b) start with three vowels?
   (c) have all letters in alphabetical order?
   (d) have all *vowels* in alphabetical order (but not necessarily beside each other)?
5. Consider the following quote:

   "You can't spell awesome without me."

   —Taylor Swift ft. Brendon Urie (2019)

   How many arrangements of the word AWESOME *do not* have the string ME?
6. Write your own problem where the ***answer*** is $\binom{7}{2}$. Be as creative as you can!
7. Determine the coefficient of the term x^3y^2 in each product:
   (a) $(x+y)^5$
   (b) $(3x+2y)^5$
   (c) $(2x-y)^5$
   (d) $(7x+7y)^5$
8. Given a standard deck of cards (see Example 2.2.17), a **straight** is a hand of five different ranks in consecutive order. For example:

   4♢ 5♡ 6♠ 7♣ 8♢.

   Assume that straights can start with an ace (A-2-3-4-5) or 10 (10-J-Q-K-A) or any other numbered card, but not with any face card (J, Q, or K). How many straights can be formed?
9. A **flush** is a hand of five cards, all of the same suit. For example, the five-card hand

   4♠ 5♠ 8♠ J♠ K♠

   is a flush.
   (a) How many flushes can be formed?

(b) How many flushes are also straights? (This hand is called a **straight flush**.)

Hint. LOL

10. A **full house** is a five-card hand with three cards of the same rank, plus two other cards of the same rank. For example, the five-card hand

7♡ 7♢ 7♣ J♡ J♠

is a full house.

How many five-card hands are full houses?

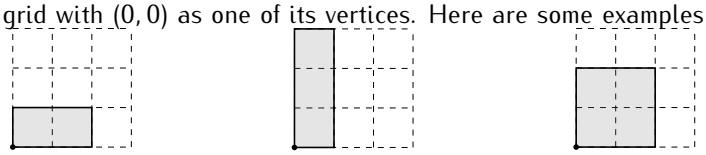
11. How many ways are there to draw a three-card hand from a standard deck of cards such that:

(a) all of them are face cards (J, Q, K)?

(b) there are at least two numbered cards?

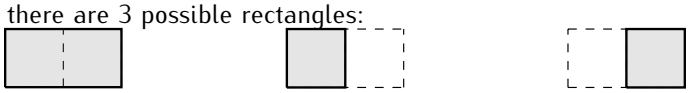
(c) there are at least two numbered cards, and exactly two red cards?

12. Count the number of rectangles that can be formed using the edges of a 3×3 grid with $(0, 0)$ as one of its vertices. Here are some examples:



13. Generalize Exercise 2.7.12 to an $m \times n$ grid.

14. Count the number of rectangles that can be formed using the edges of an $m \times n$ grid (with no restrictions on the vertices). For example, if $m = 2$ and $n = 1$, there are 3 possible rectangles:

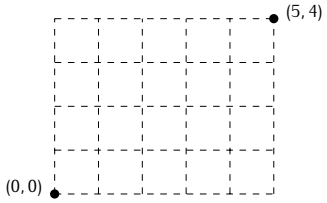


15. Count the number of lattice paths from $(0, 0)$ to $(5, 4)$ that:

(a) Pass through the point $(2, 2)$.

(b) Avoid the point $(3, 3)$.

(c) Pass through the point $(2, 2)$ *and* avoid the point *(3,3)*.



16. The Greater Toronto Area has a population of about 6 million. Suppose that each resident has a jar with 100 coins, consisting of nickels, dimes, quarters, loonies ($1), and toonies ($2). Prove that two residents must have identical jars.

17. Count the number of ways to distribute 30 identical balls into 9 different boxes so that each box is nonempty.

18. Count the number of ways $2n$ people can be grouped into pairs.

For example, when $n = 2$ and there are four people A, B, C, and D, then there are three ways to pair them up: AB/CD, AC/BD, AD/BC.

Find the number of integer solutions to each system:

19. $x_1 + x_2 + x_3 = 30$, $x_1, x_2, x_3 \geq 0$.

20. $x_1 + x_2 + x_3 + x_4 = 2020$, $x_1 \geq 30$, $x_2 \geq 40$, $x_3 \geq 50$, $x_4 \geq 100$

21. $x_1 + x_2 + x_3 + x_4 = 2020$, $x_1 \geq 300$, $x_2 \geq 400$, $x_3 \geq 500$, $x_4 \geq 1000$

22. $x_1 + x_2 + x_3 = 12$, $3 \leq x_1 \leq 5$, $1 \leq x_2$, $1 \leq x_3 \leq 7$

23. Find the number of integer solutions to

$$x_1 + x_2 - x_3 = -4$$

such that $x_1, x_2, x_3 \geq 0$ and $x_3 \leq 10$.

Hint. Let $y_3 = 10 - x_3$.

24. Find the number of nonnegative integer solutions to $x_1 + x_2 + \cdots + x_k \leq n$.

25. Prove the identity

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

by counting the number of subsets of size n of the set $\{a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n\}$.

Prove the following identities ***using combinatorial arguments***. Clearly explain which sets or objects you are counting in two ways.

26. $\displaystyle\sum_{i=1}^{n} (i-1) = \binom{n}{2}$

27. $\displaystyle\binom{2n}{n} = 2\binom{2n-1}{n-1}$

28. $\displaystyle b^3 = 6\binom{b}{3} + 6\binom{b}{2} + b$

Chapter 3

Pigeonhole and Inclusion-Exclusion

Short intro here

3.1 The Pigeonhole Principle

Objectives

- State the Pigeonhole Principle and prove the generalized version.
- Identify the pigeons and pigeonholes in a given problem and apply the Pigeonhole Principle to come to a conclusion.

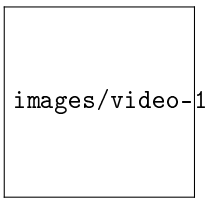
Let's kick off this chapter with a claim that seems suspect:

Claim. There are two people in Toronto with the exact same number of hair follicles on their head.

In your mind you're probably going '*Even if this were true... how would we prove it??*' And yes, we wouldn't be able to actually *count* the number of hair follicles on anyone's head. But the beauty of the Pigeonhole Principle is that we don't need to!

I'm going to let Kyne of Canada's Drag Race Season 1 explain why this claim holds true.

> Kyne was a contestant on the first season of Canada's Drag Race, and is a mathematical finance major at the University of Waterloo.



As you've seen, the Pigeonhole Principle is not a *counting* technique *per se*, but a way to prove that a set of objects satisfies some existence or extremal property. Before we state the principle formally let's look at two more examples.

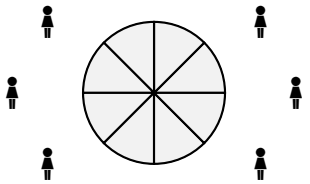
Example 3.1.1 Splitting a Pizza.

If six friends order and finish eating a pizza that is divided into 8 slices, show that one of them gets at least 2 slices.

Solution. Towards a contradiction, suppose that each person gets at most one slice only. Then they will eat at most only 6 slices among them, leaving the pizza unfinished. This is a contradiction, so there must be one person who eats at least two slices.

Observe that this proof does not deny the possibility of multiple people getting two slices: it is quite possible that four of the friends ate a slice each, and the two others ate two slices each. It is also possible that one person ate three slices, while the five remaining friends ate a slice each.

In either case, one person ate at least two slices.



That's one big pizza!

Example 3.1.2 Quiz Scores.

A class of 20 students got their quiz scores back, and their instructor told them the average for the test was 8 out of a maximum of 10. Prove that someone in the class must have scored at least an 8/10.

Solution. Denote the scores of the students by x_1, x_2, and so on until x_{20}.

Assume that nobody scored at least an 8/10; that is, $x_i < 8$ for all $i = 1, 2, \ldots, 20$. Adding all these inequalities and dividing by 20, we obtain

$$\begin{aligned} & x_1 + x_2 + \cdots + x_{20} < 160 \\ \Rightarrow \quad & \frac{x_1 + x_2 + \cdots + x_{20}}{20} < \frac{160}{20} \\ & \Rightarrow \text{class average} < 8, \end{aligned}$$

which contradicts the assumption that the average was 8 out of 10.

For the previous examples, we argued that *there is no other way* but for the required property to hold, regardless of how the pizza slices/points are actually distributed among people. We call this kind of proof a **non-constructive proof** or an **existence proof**, since it shows that the property holds without actually giving an example (or an algorithm to create an example). Like the hair follicle example, this is typical of proofs that utilize the Pigeonhole Principle.

Theorem 3.1.3 Pigeonhole Principle (PHP).

Placing more than kn objects (pigeons) into n classes (pigeonholes) puts more than k objects into some class.

Checkpoint 3.1.4 Prove the PHP. Prove Theorem 3.1.3 following the proofs of Example 3.1.1 and Example 3.1.2.

Setting $k = 1$ in the statement of the principle results in the classic version:

Corollary 3.1.5 Pigeonhole Principle with $k = 1$.

If more than n objects are placed into n classes, then some class must have at least 2 objects.

Checkpoint 3.1.6 Same Last Digit. Given any set of eleven natural numbers, prove that there must be two of them with the same last digit.

Hint. How many digits are possible?

Checkpoint 3.1.7 Difference Divisible by 10. Given any set of eleven natural numbers, prove that there must be a pair of elements whose difference is divisible by 10.

Hint. Use Checkpoint 3.1.6.

Often it is not immediately obvious what the pigeons and pigeonholes should be when we attempt to apply Theorem 3.1.3 to a problem. Moreover one needs also to give a rule that assigns pigeons to pigeonholes, such that:

- There are fewer pigeonholes (n) than pigeons ($> kn$).
- The desired property is satisfied when more than k objects is put into any class.

When using Theorem 3.1.3 one must explicitly state what the pigeons and pigeonholes are, and explain how the assignment is done.

Example 3.1.8 Sum to 8.

If five numbers are selected from the set $\{1, 2, 3, 4, 5, 6, 7\}$, prove that two of these numbers must sum to 8.

Solution. Define pigeonholes to be the sets $\{1, 7\}$, $\{2, 6\}$, $\{3, 5\}$, $\{4\}$, and pigeons to be the five numbers selected. Then picking five numbers from $\{1, 2, \ldots, 7\}$ is the same as placing 5 pigeons into these 4 pigeonholes.

$$\underline{\quad\{1,7\}\quad} \quad \underline{\quad\{2,6\}\quad} \quad \underline{\quad\{3,5\}\quad} \quad \underline{\quad\{4\}\quad}$$

Note that the last pigeonhole by definition can only contain at most one pigeon—this does not affect the proof. By PHP, there is a pigeonhole with two pigeons. That is, two numbers are selected from one of these sets; these two numbers must sum to 8.

We say that the number five is **best possible** in Example 3.1.8 since it is possible to select four numbers and not have any pair sum to 8 (for instance, pick 1, 2, 3, and 4). But selecting *any* five numbers from $\{1, 2, \ldots, 7\}$ guarantees the property is satisfied.

Checkpoint 3.1.9 Sum to $2n$. Generalize Example 3.1.8. That is, if $n+1$ numbers are selected from the set $\{1, 2, \ldots, 2n-1\}$, prove that two of these numbers must sum to $2n$.

The next example is slightly different in that we're not given a fixed set of numbers to work with. Instead, the result being proven holds for any set of six integers. (Convince yourself it works and try proving it yourself first before expanding the solution!)

Example 3.1.10 Sum or Difference Divisible by 8.

Given *any* set of six integers, show that there is a pair among them whose sum *or* difference is divisible by 8.

Hint. Use remainders modulo 8.

Solution. If a pair of integers a, b among the six have the same remainder when dividing by 8, then their difference $a - b$ is divisible by 8, and we are done.

So assume that all six integers have distinct remainders when dividing by 8. Construct the five pigeonholes $\{0\}, \{1,7\}, \{2,6\}, \{3,5\}, \{4\}$ and place each of the six numbers in the pigeonhole corresponding to its remainder.

By PHP, one of these pigeonholes must have two numbers. That is, summing those two numbers gives a sum that is divisible by 8.

Checkpoint 3.1.11 Six is Best Possible. Show that Example 3.1.10 is best possible by constructing a set of five integers for which *no pair* has sum or difference divisible by 8.

Checkpoint 3.1.12 Sum or Difference Divisible by $2n$. Prove this generalization of Example 3.1.10:

Given any set of $n + 2$ integers, there is a pair among them whose sum or difference is divisible by $2n$.

A few more applications to conclude this section.

Example 3.1.13 Number of Friends.

Prove that in any group of people, there must be two of them with the same number of friends in the group.

Solution. Suppose there are n people in the group. Then each person can have $0, 1, \ldots,$ or $n - 1$ friends among the group. This is still n pigeonholes, so we cannot apply PHP yet.

Observe that it cannot happen that someone has no friends, and someone else has $n-1$ friends. (If a person has $n-1$ friends, then every other person has at least one friend.) Hence there are only $n - 1$ possible numbers of friends among the n people, which means two of them must have the same number of friends, by the PHP.

Checkpoint 3.1.14 One Divides Another. Prove that any $(n + 1)$-subset of $\{1, 2, \ldots, 2n\}$ contains two numbers such that one divides the other.

Hint. Pigeonholes are $\{1\}, \{3\}, \{5\}, \ldots, \{2n - 1\}$; assign each number to the pigeonhole that contains its largest odd divisor. If two numbers are in the same pigeonhole, why should one divide the other?

Checkpoint 3.1.15 Tracking Showers. Over a two-week period (14 days), you kept track of how many showers you took. Your records show that you showered at least once every day, and that you showered a total of 17 times.

By following the steps below, prove that there was a period of consecutive days during which you showered exactly 10 times.

(a) Define variables x_i to be the number of times you took a shower on day i $(1 \leq i \leq 14)$, and define $y_i = x_1 + x_2 + \cdots + x_i$ to be the partial sums. Explain why it suffices to prove $y_i = y_j + 10$ for some i, j.

(b) Explain why the set

$$\{y_1, y_2, \ldots, y_{14}, y_1 + 10, y_2 + 10, \ldots, y_{14} + 10\}$$

can only contain numbers from 1 to 27.

(c) Apply Theorem 3.1.3 to prove the desired property. What are the pigeons and pigeonholes?

3.2▲ Principle of Inclusion-Exclusion

Objectives

- State the Principle of Inclusion-Exclusion and apply it to problems to compute set cardinalities (for combinations of two to four sets).
- Sketch Venn Diagrams that correspond to a given scenario or problem.

We first recall that in order to count the number of elements of a set U that *don't* satisfy a given condition, one can first count the number of elements that *do*, and then subtract from the cardinality of U.

Example 3.2.1 Not Divisible by 3.

How many integers in $U = \{1, 2, \ldots, 25\}$ are *not* divisible by 3?

Solution We first count the number of integers in the set that are divisible by 3: there are

$$\left\lfloor \frac{25}{3} \right\rfloor = 8$$

of them.

Note that the notation $\lfloor n \rfloor$ denotes the **floor function**, which returns the largest integer that is less than or equal to n.

Subtracting, we get $25 - 8 = 17$ integers in the set U that are not divisible by 3. (Check that this is the correct number!)

Note that this solution can be expressed in terms of sets: if $U = \{1, 2, \ldots, 25\}$ is the universe, and A is the set of integers in U divisible by 3, then the desired quantity is $|A^c|$, and

$$|A^c| = |U| - |A|.$$

What if we added a second condition to avoid?

Example 3.2.2 Not Divisible by 3 or 4.

How many numbers in $U = \{1, 2, \ldots, 25\}$ are not divisible by 3 or 4?

Solution. Following the previous example, there are 8 integers in U that are divisible by 3. Also, there are $\lfloor \frac{25}{4} \rfloor = 6$ integers in U not divisible by 4.

However, after subtracting $25 - 8 - 6 = 11$, we've actually removed some numbers twice: those numbers that are divisible by *both* 3 and 4 (i.e. divisible by 12). This means we need to 'add them back in' again.

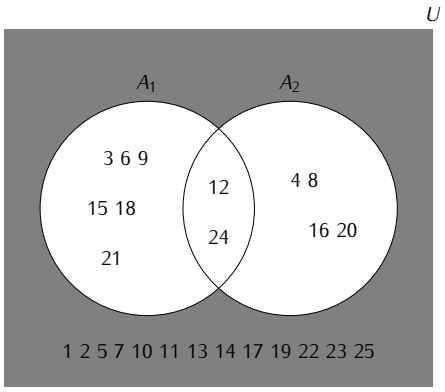
There are $\lfloor \frac{25}{12} \rfloor = 2$ of these numbers, so the correct total is

$$20 - 8 - 6 + 2 = 13$$

integers in the set that are neither divisible by 3 nor by 4.

We can again write the solution to Example 3.2.2 in terms of sets:

- $U = \{1, 2, \ldots, 25\}$
- $A_1 =$ integers in U divisible by $3 = \{3, 6, 9, 12, 15, 18, 21, 24\}$
- $A_2 =$ integers in U divisible by $4 = \{4, 8, 12, 16, 20, 24\}$
- $A_1 \cup A_2 =$ integers in U divisible by either 3 or $4 = \{3, 4, 6, 8, 9, 12, 15, 16, 18, 20, 21, 24\}$
- Desired set: $(A_1 \cup A_2)^c =$ integers in U divisible by neither 3 nor 4.



Observe that when we subtract $|A_1|$ and $|A_2|$ from $|U|$, we are subtracting the elements in the intersection $A_1 \cap A_2 = \{12, 24\}$ two times. So to determine the quantity $|(A_1 \cup A_2)^c|$ we computed:

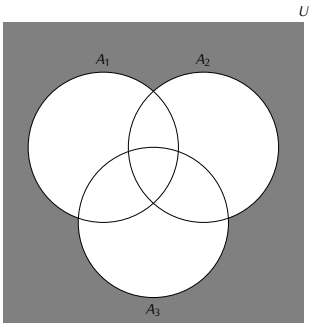
$$|(A_1 \cup A_2)^c| = |U| - |A_1| - |A_2| + |A_1 \cap A_2|.$$

Remark 3.2.3

Do not confuse the operations $|A| - |B|$ and $A \setminus B$. The first is a difference of two numbers, while the second is a set operation that also results in a set. In fact, it is not the case that $|A| - |B| = |A \setminus B|$ in general. (Can you come up with a counterexample?)

Checkpoint 3.2.4 Not Divisible by 7 or 11. How many integers in $\{1, 2, 3, \ldots, 2020\}$ are not divisible by 7 or 11?

Now suppose we add a third condition to avoid, that is, a third set A_3 to remove. Consider the problem of determining the number of elements in the set $(A_1 \cup A_2 \cup A_3)^c$.



The idea now is to replicate the 2-set scenario by first subtracting $|A_1| + |A_2| + |A_3|$ from $|U|$, then to add back what was removed more than once. This means we have to add back $|A_1 \cap A_2|$, $|A_1 \cap A_3|$, and $|A_2 \cap A_3|$.

However, elements in the intersection of all three sets $A_1 \cap A_2 \cap A_3$ have been removed three times and added back three times at this point. This means we should subtract

$$|A_1 \cap A_2 \cap A_3|$$

one more time so that we remove all the elements we need to remove.

To summarize: (note the alternating signs)

$$|(A_1 \cup A_2 \cup A_3)^c| = |U| \underbrace{-|A_1| - |A_2| - |A_3|}_{\text{single sets}} \underbrace{+|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|}_{\text{intersections of pairs}} \underbrace{-|A_1 \cap A_2 \cap A_3|}_{\text{intersection of all three}}.$$

Checkpoint 3.2.5 Not Divisible by 3, 7, or 11. How many integers in $\{1, 2, \ldots, 2020\}$ are not divisible by 3, 7, or 11?

Now we can state the Principle of Inclusion-Exclusion (or PIE) in full generality. There are a number of ways to prove this, but the usual method is to show that each item belonging to none of the A_i's contribute 1 to the total; while all other items contribute 0 to the total.

Theorem 3.2.6 Principle of Inclusion-Exclusion.

Given a universe U of items and subsets $A_1, A_2, \ldots, A_n$ of the items, the number N of items belonging to none of these subsets *is given by*

$$\begin{aligned} N &= \sum_{S \subseteq \{1,2,\ldots,n\}} (-1)^{|S|} \left| \bigcap_{i \in S} A_i \right| \\ &= |U| - \sum_{i=1}^{n} |A_i| + \sum_{1 \le i < j \le n} |A_i \cap A_j| - \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| + \cdots \end{aligned}$$

Proof. Suppose that the element x is in none of the A_i's. Then it is counted exactly once in the sum, in the first term $|U|$.

Now suppose that the element y is in some collection of A_i's. Let $T = \{i : y \in A_i\}$ be the set of indices of sets that contain y. (For example, if y is in A_1, A_3, and A_4, then $T = \{1, 3, 4\}$.) Then for each subset S of T, there is a corresponding term in the formula above.

Note that the formula contributes a $+1$ for intersections of even numbers of sets (or for $|S|$ even); and a -1 for intersections of odd numbers of sets (for $|S|$ odd). Hence the total contribution for the element y is

$$\sum_{S \subseteq T} (-1)^{|S|} = \sum_{k=0}^{|T|} (-1)^k \binom{|T|}{k}.$$

Applying Theorem 2.3.5, we see that this is equal to

$$\sum_{k=0}^{|T|} (-1)^k \binom{|T|}{k} = \sum_{k=0}^{|T|} (1)^{|T|-k} (-1)^k \binom{|T|}{k} = (1 + (-1))^{|T|} = 0,$$

which is what we needed to prove.

Checkpoint 3.2.7 PIE for Four Sets. Given a universe U and four sets A_1, A_2, A_3, A_4 in U, write out the complete formula for $|(A_1 \cup A_2 \cup A_3 \cup A_4)^c|$.

Example 3.2.8 Word Rearrangements.

Count the number of arrangements of the letters in the word
EQUATION
such that

- vowels are *not* in alphabetical order when read left-to-right; ***and***
- consontants are *not* in alphabetical order when read left-to-right.

Solution. Let A_1 be the set of arrangements where vowels are in alphabetical order, and A_2 the set of arrangements where consonants are in alphabetical order. Then the desired number is $|(A_1 \cup A_2)^c| = |U| - |A_1| - |A_2| + |A_1 \cap A_2|$, by Theorem 3.2.6.

We compute each quantity:

- $|U| = 8!$, the number of permutations of the letters.
- $|A_1| = 3! \cdot \binom{8}{3}$ (permute the consonants first, then insert among vowels using the Balls in Bins Formula)
- $|A_2| = 5! \cdot \binom{8}{5}$ (permute the vowels first, then insert among consontants)
- $|A_1 \cap A_2| = \binom{8}{5}$ (vowels and consonants are in a fixed order; just pick 5 slots for vowels to be in and the rest follows)

Hence $|(A_1 \cup A_2)^c| = |U| - |A_1| - |A_2| + |A_1 \cap A_2| = 8! - 3!\binom{8}{3} - 5!\binom{8}{5} + \binom{8}{5}$, or 33320.

Checkpoint 3.2.9 Relatively Prime Numbers. Use Theorem 3.2.6 to determine how many natural numbers less than 120 are relatively prime with 120.

Hint. Consider prime factors of 120.

Exploration 3.2.1 Euler's Totient Function.

Given $n \in \mathbb{N}$ and $\{p_1, p_2, \ldots, p_k\}$ its set of prime factors, we will prove the following formula for the number of natural numbers less than n (denoted by $\phi(n)$) that are also relatively prime with n:

$$\phi(n) = \sum_{S \subseteq \{1,2,\ldots,k\}} (-1)^{|S|} \frac{n}{\prod_{i \in S} p_i}.$$

(This is known as **Euler's totient function**.)

(a) Define A_i to be the set of natural numbers less than n that are divisible by p_i. Compute the value of $|A_i|$.

Hint. Example 3.2.1.

(b) For any set $S \subseteq \{1, 2, \ldots, k\}$, compute the value of $\left|\bigcap_{i \in S} A_i\right|$.

(c) Express $\phi(n)$ as a combination of the sets A_i and apply Theorem 3.2.6 to obtain the desired formula.

Checkpoint 3.2.10 Compute $\phi(100)$ and $\phi(135)$. Use the formula in Exploration 3.2.1 to compute $\phi(100)$ and $\phi(135)$.

Checkpoint 3.2.11 One Card of Each Suit. Use Theorem 3.2.6 to determine how many five-card hands can be drawn from a standard deck of cards such that there is at least one card of each suit.

Checkpoint 3.2.12 Nonnegative Integer Solutions. Use Theorem 3.2.6 to determine how many nonnegative integer solutions there are to $x_1 + x_2 + x_3 = 10$, $x_1 \leq 3$, $x_2 \leq 4$, $x_3 \leq 8$.

Hint. Define A_1 to be the set of solutions such that $x_1 > 3$, etc.

3.3▲ Application: Derangements

Objectives

- Define derangements and use the Principle of Inclusion-Exclusion to derive a general formula for them.
- Recognize scenarios where derangements apply and use them to solve problems.

Recall that the permutations of a set S are the bijective functions from S to itself. We have a special name for those permutations that leave no element fixed:

Definition 3.3.1 Derangement.

A **derangement** is a permutation on $\{1, 2, \ldots, n\}$ such that no element is mapped to itself.

Example 3.3.2 Derangements of 3- and 4-sets.

The permutation on $\{1, 2, 3\}$ that takes 1 to 3, 2 to 1, and 3 to 2 is a derangement; we can also denote it as the string 312.

There are only two derangements on $\{1, 2, 3\}$: 231 and 312.

The permutation 3241 on $\{1, 2, 3, 4\}$ is *not* a derangement since 2 is sent to itself. We call 2 a **fixed point** of the permutation.

(Try listing all derangements of $\{1, 2, 3, 4\}$.)

Exploration 3.3.1 Deriving D_n.

Count the number of derangements D_n of the set $\{1, 2, \ldots, n\}$ using Theorem 3.2.6, by following these steps:

(a) Define A_i to be the set of permutations of $\{1, 2, \ldots, n\}$ for which i is a fixed point. (There are no restrictions on the other elements; there may be other fixed points.)

Then, express D_n as the cardinality of a set involving the A_i's.

(b) If $S \subseteq \{1, 2, \ldots, n\}$ with $|S| = k$, find a formula for $\left|\bigcap_{i \in S} A_i\right|$.

(c) Combine with Theorem 3.2.6 to derive a formula for D_n, then fill in the statement of the result below.

Theorem 3.3.3 Number D_n of Derangements.

The number of derangements D_n of the set $\{1, 2, \ldots, n\}$ is

$$D_n = \_\_\_\_\_ .$$

Remark 3.3.4

For problems where it is relevant, you may leave your answers in terms of D_n. (You don't have to compute exact values unless asked.)

Checkpoint 3.3.5 Compute D_4. Evaluate D_4 and verify that it is the correct number by listing all derangements of $\{1, 2, 3, 4\}$.

Checkpoint 3.3.6 The Ratio $D_n/n!$ Using a computer, evaluate the ratio

$$\frac{D_n}{n!}$$

of derangements to all permutations of $\{1, 2, \ldots, n\}$ for n increasingly large.

Verify that the ratios approach the value of $\frac{1}{e}$.

3.4▲ Exercises

Additional Exercises for Chapter 3

1. Prove that any $(n+1)$-subset of $\{1, 2, \ldots, 2n\}$ has a pair of consecutive numbers.

   Why does this imply that any $(n+1)$-subset must have a pair of relatively prime numbers?

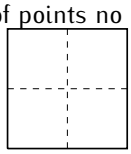
2. Prove that any $(2n+1)$-subset of $\{1, 2, \ldots, 3n\}$ has three consecutive numbers.

3. The numbers 1 to 10 are placed in some order around a circle. Prove that some set of three consecutive numbers sums to at least 17.

   Hint. What should the average of all the three-sums be?

4. Jungkook has 6 friends; over several days he invites some of them over to his home to eat lamb skewers for dinner, so that the company never repeats (i.e. a different set of friends comes every night). If he has at least one friend over every day, how many days can he follow this rule?

5. Place 5 points inside (or on the boundary) of a square with side length 2 cm. Show that there is a pair of points no more than $\sqrt{2}$ cm apart.



6. Recall that the **midpoint** of the segment joining points (a, b) and (c, d) on the plane has coordinates

$$\left(\frac{a+c}{2}, \frac{b+d}{2}\right).$$

   Show that given five integer points (i.e. points with integer coordinates) on the plane, the midpoint of the segment joining some pair of them is also an

integer point.

Hint. Consider parity.

7. If we select 38 subsets of size at most three from the set $S = \{1, 2, \ldots, 13\}$, show that two of these subsets must have the same sum.

8. The UTM e-sports team *Eagle Geniuses* is training for an Ontario e-sports tournament called *The Provincial*, which is 30 days away. They are scheduled to play at least one scrim (practice game) with another university team every day for the next 30 days; their coach tells them they will be playing a total of 42 games.

Prove that there was a period of consecutive days during which the team scrimmed exactly 17 times.

Hint. Similar to Checkpoint 3.1.15.

9. Fall 2020 course data about 1000 first-year students at a college reveal that:

- 800 are taking calculus
- 750 are taking linear algebra
- 550 are taking an intro to proofs course
- 650 are taking calculus and linear algebra
- 500 are taking linear algebra and proofs
- 500 are taking calculus and proofs
- 450 are taking all three

(a) How many students are taking none of these courses?

(b) How many students are taking only linear algebra?

(c) Draw a venn diagram and indicate the number of students for each part of the diagram.

10. How many ways are there to place 11 distinct people into 3 distinct rooms?

How many ways are there to place 11 distinct people into 3 distinct rooms such that each room has at least one person?

11. Twenty students in a class exchange quiz papers for peer evaluation. How many ways can this be done so that no student gets their own paper?

12. Count the number of 5-letter arrangements that can be formed from the letters of the word

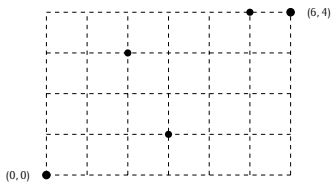
EUPHORIA

such that the string EAR does not appear, and there is at least one vowel.

13. Count the number of integer solutions to the system

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 25 \\ 2 \leq x_1 \leq 9 \\ 3 \leq x_2 \leq 9 \\ -1 \leq x_3 \leq 11 \\ 5 \leq x_4 \end{cases}$$

14. Count the number of lattice paths from $(0, 0)$ to $(6, 4)$ that pass through *at least one* of the points $(2, 3)$, $(3, 1)$, and $(5, 4)$.



15. Consider a set of n cats and n dogs; suppose we want to pair them up for an afternoon playdate. Derive formulas for the number of ways this can be done, such that:

(a) For each i, the ith heaviest cat is *not* paired up with the ith heaviest dog (but pairs can have two dogs or two cats).

(b) Same condition as (a), but also each pair has exactly one cat and one dog.

16. Suppose that four friends have two pets each—a cat and a dog—and they all meet up at the park. They decide to form four groups of one human, one cat, and one dog each. Count the number of ways they can do this, such that:

(a) No human is with their dog.

(b) No human is with either of their pets.

(c) Each human is grouped with at most one of their pets.

Chapter 4

Congruence Modulo n

4.1 ▲ Equivalence Relations

Objectives

- Define relations on a set; determine whether or not a relation is an equivalence relation; determine the congruence classes of equivalence relations
- Construct proofs about relations and their properties.

You will have seen equivalence relations in MAT102. Recall that they allow us to talk about the *same-ness* of objects in terms of some defining characteristic, even if those two objects are not necessarily *equal*.

Relations generalize functions; equivalence relations are relations that satisfy a number of properties.

Definition 4.1.1 Relation.

Given sets S and T, a **relation** between S and T is a subset of $S \times T$; that is, R is a relation if $R \subseteq S \times T$.

If $S = T$ then we call R a **relation on** S.

Example 4.1.2 A Simple Relation.

Let $A = \{0, 2, 4, 6\}$ and $B = \{0, 1, 2, 3, 4\}$.

The set

$$R = \{(0, 0), (0, 2), (2, 2), (6, 3), (6, 4)\}$$

is a subset of $A \times B$, so R is a relation between A and B.

Checkpoint 4.1.3 Counting Relations. How many relations are there between the sets $A = \{0, 2, 4, 6\}$ and $B = \{0, 1, 2, 3, 4\}$?

Hint. How many subsets does $A \times B$ have?

Checkpoint 4.1.4 Counting Relations and Functions. Let A and B be finite sets.

(a) How many relations are there between A and B?

(b) How many *functions* are there from A to B?

Which of your anwers from (a) or (b) should be larger? Why?

Equivalence relations are a special type of relation—they satisfy a number of additional conditions that allow for a reasonable way to talk about objects being *equivalent*.

Definition 4.1.5 Equivalence Relation.

An **equivalence relation** R on a set S is a relation such that

Reflexive property For all $x \in S$, $(x, x) \in R$.

Symmetric property For all $x, y \in S$, $(x, y) \in R$ implies $(y, x) \in R$.

Transitive property For all $x, y, z \in S$, $(x, y) \in R$ and $(y, z) \in R$ imply $(x, z) \in R$.

Checkpoint 4.1.6 Equivalence Relation or Not? For each relation, determine whether or not it satisfies the reflexive, symmetric, and transitive properties. Then conclude whether or not it is an equivalence relation.

(a) The order relation $<$ on $\mathbb{R}$

(b) The relation $R = \{(a, a), (b, b), (c, c), (a, b), (b, a), (a, c), (c, a)\}$ on the set $\{a, b, c\}$

(c) The relation $D = \{(m, n) : m + n \text{ is odd}\}$ on $\mathbb{Z}$

(d) The relation $\equiv$ on $\mathbb{Z}$ given by $a \equiv b \iff n \mid (a - b)$, for a fixed $n \in \mathbb{N}$

(e) The relation $\sim$ on $\mathbb{R}$ given by $x \sim y \Leftrightarrow (x - y)(x^2 + y^2 - 1) = 0$

(f) The relation $\approx$ on $\mathbb{R}^2$ given by $(x, y) \approx (w, z) \Leftrightarrow xy = wz$

Definition 4.1.7 Equivalence Class.

Let R be an equivalence relation on a set S, and x an element in S.

The **equivalence class** of x, denoted by $[x]$, is the set of all elements in S related to x under R; that is,

$$[x] = \{y \in S : (x, y) \in R\}.$$

Checkpoint 4.1.8 List the Equivalence Classes. List all equivalence classes of the equivalence relation

$$R = \{(v, v), (w, w), (x, x), (y, y), (z, z), (v, z), (z, v), (w, x), (x, w), (y, y)\}$$

on the set $S = \{v, w, x, y, z\}$.

An equivalence relation on a set S induces a partition of S into its equivalence classes. This is shown by proving that none of the equivalence classes overlap, and that their union is S. First, we prove the following lemma that states that if two elements are equivalent, then their equivalence classes are equal. Note the extra care in using the equivalence relation properties.

Lemma 4.1.9 Equivalent Objects are in the Same Class.

Let R be an equivalence relation on S, and let $a, b \in S$. If $(a, b) \in R$, then $[a] = [b]$.

Proof. Let R be an equivalence relation on S, and let $a, b \in S$ such that $(a, b) \in R$. We will prove $[a] \subseteq [b]$.

Let $y \in [a]$. Then:

$$\begin{aligned} (a, y) &\in R && \text{(by definition of } [a]) \\ (y, a) &\in R && \text{(since } R \text{ is symmetric)} \\ (a, b) &\in R && \text{(given)} \\ (y, b) &\in R && \text{(since } R \text{ is transitive)} \\ (b, y) &\in R && \text{(since } R \text{ is symmetric)} \\ y &\in [b] && \text{(by definition of } [b]) \end{aligned}$$

Hence $[a] \subseteq [b]$. The other inclusion is similarly proved, from which $[a] = [b]$ follows.

Theorem 4.1.10 Equivalence Relations induce Partitions.

If R is an equivalence relation on a set S, then

(a) any $x \in S$ belongs to some equivalence class; and

(b) any two different equivalence classes are disjoint.

In particular, the equivalence classes induced by R form a partition of the set S.

Checkpoint 4.1.11 Prove Theorem 4.1.10 (a). Write a one-line proof of part (a) of Theorem 4.1.10.

Checkpoint 4.1.12 Prove Theorem 4.1.10 (b). Prove part (b) of Theorem 4.1.10 by showing that any two equivalence classes that have a common element must be the same equivalence class.

Hint. You may want to use Lemma 4.1.9.

Checkpoint 4.1.13 Describe the Classes I. Describe the equivalence classes of the equivalence relation $\sim$ on $\mathbb{Z}$ defined by

$$m \sim n \Leftrightarrow 3 \mid (m - n).$$

Checkpoint 4.1.14 Describe the Classes II. Let $A = \{0, 1, 2\}$, and consider the relation $\cong$ on $P(A)$ defined by

$$X \cong Y \Leftrightarrow \text{ the largest element in } X \text{ equals the largest element in } Y.$$

Prove $\cong$ is an equivalence relation, and describe the equivalence classes.

Checkpoint 4.1.15 Give Examples. Give examples of equivalence relations on $\mathbb{Z}$:

(a) with exactly one equivalence class;

(b) with exactly two equivalence classes;

(c) with infinitely many equivalence classes.

Remark 4.1.16 Representatives of Equivalence Classes.

If x and y are in the same equivalence class, then $[x] = [y]$, and we can use either of them to refer to the same class. In fact, we can use any member of the class to represent it!

Example 4.1.17 Multiple Possible Representatives.

Consider the equivalence relation

$$E = \{(a, b) : a + b \text{ is even}\}$$

on $\mathbb{Z}$.

The equivalence class of 0 is

$$[0] = \{a : a + 0 \text{ is even}\} = \{a : a \text{ is even}\},$$

and hence $[0]$ contains exactly all even integers. This means we can also call $[0]$ as $[2] = [-2] = [4] = \cdots$ (any of these names).

Similarly,

$$[1] = \{a : a + 1 \text{ is even}\} = \{a : a \text{ is odd}\}.$$

So, $[1] = [-1] = [3] = [-3] = [5] = \cdots$.

We can use the properties of equivalence classes and the additional results we've proven to derive interesting consequences about equivalence relations. For instance, if two objects are in the same equivalence class, then they must be equivalent to one another. (This sounds obvious—try to prove it below!)

Checkpoint 4.1.18 Objects in the Same Class are Equivalent. Given an equivalence relation R on a set S, and an equivalence class $[x]$, show that for all $a, b \in S$,

$$a \in [x] \text{ and } b \in [x] \Rightarrow (a, b) \in R.$$

4.1.1 ▸▸ Solutions to Selected Checkpoints

4.2▲ Congruences and their Properties

Objectives

- Define congruence modulo n and show it is an equivalence relation.
- Prove properties about congruence relations.

In part (d) of Checkpoint 4.1.6 you would have proven that $\equiv$ was an equivalence relation on the integers. This is an important relation that has several applications, so it is given a name.

Definition 4.2.1 Congruence.

Let n be a natural number. We say that two integers a and b are **congruent modulo** n if $n \mid (a - b)$. We denote this by writing

$$a \equiv b \pmod{n}.$$

The number n is called the **modulus**.

Example 4.2.2 Simple Example.

Since $6 \mid (55 - 13)$, 55 and 13 are congruent modulo 6, and we write $55 \equiv 13 \pmod 6$.

However $6 \nmid (30 - 11)$ so 30 and 11 are *not* congruent modulo 6, or $30 \not\equiv 11 \pmod 6$.

Checkpoint 4.2.3 Congruent iff Same Remainder. Show that two integers a and b are congruent modulo n if and only if they have the same remainder when divided by n.

Hint. Use Theorem 1.3.2.

One real-life example is that of computing what day of the week it is, which uses congruence modulo 7.

Example 4.2.4 Days of the Week.

Modulo 7, the numbers 26 and 47 are congruent because $7 \mid (26 - 47)$. This means 26 and 47 are 'equivalent' under this particular relation.

One way to see this is the fact that if today were Sunday, then 26 days from today it will be Friday, and 47 days from today is also a Friday. Abstracting only the property we care about (remainder when divided by 7) allows us to generate conclusions like this without having to manually count 47 days forward.

As another example, if today were Sunday, then we can confidently claim that 2020 days from today, it will be Thursday. This is because $2020 \equiv 4 \pmod 7$, and four days after Sunday is Thursday. (We've effectively removed as many 7's as possible to reduce the calculation.)

Checkpoint 4.2.5 New Relationship. Today, two of your friends bought each other matching couple shirts to celebrate being in a relationship for 100 days. If today is Wednesday, what day did their relationship begin?

Definition 4.2.6 Congruence Class.

The equivalence classes of congruence modulo n are called **congruence classes** or **remainder classes**, and they are the sets

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\},$$

corresponding to the possible remainders when dividing by n.

Example 4.2.7 Modulo 5.

Modulo 5, the congruence classes are

$$\begin{aligned}
[0] &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\
[1] &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\
[2] &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\
[3] &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\
[4] &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}
\end{aligned}$$

Observe that if two numbers a and b are congruent modulo n, then their difference $a - b$ is congruent to 0 modulo n. This is because a and b are

essentially *the same* when working modulo n (the remainder is all that matters), so subtracting them will give '0' in that framework.

We can perform addition and multiplication modulo n as well.

Proposition 4.2.8 Modular Arithmetic.

Let n be a natural number, and a, b, r, s integers such that $a \equiv r \pmod{n}$ and $b \equiv s \pmod{n}$. Then:

(a) $a + b \equiv r + s \pmod{n}$.

(b) $ab \equiv rs \pmod{n}$.

(c) $a^k \equiv r^k \pmod{n}$ *for any* $k \in \mathbb{N}$.

Checkpoint 4.2.9 prove Proposition 4.2.8. Prove Proposition 4.2.8.

Importantly, Proposition 4.2.8 implies that in any congruence, we can replace any number with another number it is congruent to, and obtain an equivalent statement.

Example 4.2.10 Substituting Congruent Numbers.

Suppose we wanted to compute the remainder when 4133 is divided by 4. We first write $4133 = 4000 + 100 + 30 + 3$, so that

$$4000 + 100 + 30 + 3 \equiv 0 + 0 + 2 + 3 \pmod{4} \equiv 1 \pmod{4}.$$

Hence the remainder when 4133 is divided by 4 is 1.

Definition 4.2.11 The Modulo Operation.

Given two integers a and m, with $m \neq 0$, the **modulo operation** denoted by

$$a \textbf{ mod } m,$$

read as *a modulo m*, is the remainder obtained from Theorem 1.3.2 when a is divided by m.

Checkpoint 4.2.12 Compute Remainders. Compute the following:

(a) 2139138 **mod** 9

(b) 2^{1000} **mod** 7

(c) $10!$ **mod** 17

While Proposition 4.2.8 allows us to perform addition, subtraction and multiplication, when we try dividing we find that we run into some issues.

Example 4.2.13 Division is not as Nice.

We know that

$$39 \equiv 123 \pmod{12}.$$

If we divide both sides by 3, we would get

$$13 \equiv 41 \pmod{12},$$

which is *false*. However $13 \equiv 41 \pmod{4}$ is true.

Proposition 4.2.14 Dividing both sides of a Congruence.

Let $n \in \mathbb{N}$ and $a, b, d \in \mathbb{Z}$. If $ad \equiv bd \pmod{n}$, then

$$a \equiv b \left(\mod \frac{n}{\gcd(d,n)}\right).$$

If d and n are relatively prime, then $ad \equiv bd \pmod{n}$ implies

$$a \equiv b \pmod{n}.$$

Proof. Suppose that $ad \equiv bd \pmod{n}$. This means $ad = bd + kn$ for some $k \in \mathbb{Z}$.

Since $\gcd(d,n)$ divides both d and n, we can divide through to get

$$a \cdot \frac{d}{\gcd(d,n)} = b \cdot \frac{d}{\gcd(d,n)} + k \cdot \frac{n}{\gcd(d,n)}.$$

This is equivalent to

$$\frac{n}{\gcd(d,n)} \,\Big|\, (a-b)\left(\frac{d}{\gcd(d,n)}\right).$$

Since $\gcd\left(\frac{d}{\gcd(d,n)}, \frac{n}{\gcd(d,n)}\right) = 1$, we can apply the result of Checkpoint 1.3.12 to obtain

$$\frac{n}{\gcd(d,n)} \,\Big|\, (a-b),$$

or that $a \equiv b \left(\mod \frac{n}{\gcd(d,n)}\right)$, as desired.

If $\gcd(d,n) = 1$, the statement reduces to $a \equiv b \pmod{n}$.

Checkpoint 4.2.15 Justify It. Explain why

$$\gcd\left(\frac{d}{\gcd(d,n)}, \frac{n}{\gcd(d,n)}\right) = 1$$

in the proof of Proposition 4.2.14.

Hint. Contradiction.

The second statement of Proposition 4.2.14 is also called the ***cancellation law***, since it gives a condition under which one can divide both sides of a congruence by a number.

4.2.1 ▸▸ Solutions to Selected Checkpoints

4.3▲ Solving Congruences

Objectives

- Determine if an integer has a multiplicative inverse, and find it if it exists.
- Solve linear congruences by using properties of congruence and/or finding the multiplicative inverse.

When we are asked to *solve for* x in an equation like $2x^2 + 4 = 36$, we know that we need to look for all values of x that satisfy that equation ($x = \pm 4$). What if we are asked to solve for x given a congruence?

Example 4.3.1 Solving for x.

Solve for x in the congruence $2x \equiv 4 \pmod 9$.

Before looking at the solution, try it yourself first! What value(s) of x will satisfy the congruence?

Solution. We need to find all values of x so that $9 \mid (2x-4)$, or $9 \mid 2(x-2)$.

Since $\gcd(2, 9) = 1$, by Checkpoint 1.3.12 we have $9 \mid (x - 2)$, which means $x \equiv 2 \pmod 9$.

Note that this is no different from applying Proposition 4.2.14 directly: since $\gcd(2, 9) = 1$, we can safely divide both sides by 2 to obtain $x \equiv 2 \pmod 9$.

This means that the congruence class $[2]$ is the solution to $2x \equiv 4 \pmod 9$, or that all integers in $\{\ldots, -16, -7, 2, 11, \ldots\}$ satisfy the congruence.

The final answer in the above example is typical of solutions to congruences: since we are working modulo n, answers will be congruence classes from $\{[0], [1], \ldots, [n-1]\}$. Hence when asked to *solve for* x given a congruence, you should express your answer as a congruence class ($[2]$), or as a statement of congruence like $x \equiv 2 \pmod 9$, which makes the modulus explicit.

Example 4.3.2 Solve for x.

Solve the congruence

$$2x \equiv 6 \pmod{10},$$

and express your answer using congruence classes of the original modulus.

Solution. We can apply Proposition 4.2.14 here to divide through by 2, and we get

$$x \equiv 3 \pmod 5.$$

Modulo 10, this is the same as

$$x \equiv 3 \pmod{10} \text{ and } x \equiv 8 \pmod{10}.$$

So the original congruence has two solutions in $\{[0], [1], \ldots, [9]\}$, namely $[3]$ and $[8]$.

Checkpoint 4.3.3 Solve Each Congruence. Solve each congruence for x, paying special attention to your usage of Proposition 4.2.14.

(a) $3x \equiv 9 \pmod{10}$

(b) $5x + 2 \equiv 27 \pmod{15}$

(c) $-11x - 3 \equiv 30 \pmod 7$

Checkpoint 4.3.4 Solve Another One. Proposition 4.2.14 cannot be used to solve the congruence

$$2x \equiv 3 \pmod 7$$

since we cannot divide both sides by 2.

Solve the congruence by trial-and-error.

Hint. There are only 7 congruence classes to check, since we are working modulo 7.

We've seen that dividing both sides by a constant is not always possible. Recall instead that in the real numbers, division by a nonzero number x is the same as multiplication by its reciprocal $\frac{1}{x}$. The number $\frac{1}{x}$ is sometimes called the *inverse* of x since they 'cancel' each other out when multplied together.

We define a similar concept for modular arithmetic.

Definition 4.3.5 Multiplicative Inverse.

Given natural numbers a, m such that $\gcd(a, m) = 1$, the number b is called a **multiplicative inverse** of a modulo m if

$$ab \equiv 1 \pmod m.$$

We can denote this inverse as $a^{-1} = b$, or by $a^{-1} \pmod m$ to make the modulus explicit.

In Definition 4.3.5 we are really saying that any number in $[b]$ is a multiplicative inverse of a modulo m, though we will usually be interested in finding that specific inverse that is also in the set $\{0, 1, \ldots, m-1\}$. This can now be used when solving congruences of the form

$$ax \equiv b \pmod n$$

where $a \nmid b$. Instead of dividing both sides by a (which can't always be done), we multiply both sides by the inverse of a.

Checkpoint 4.3.6 Checkpoint 4.3.4 Again. Show that modulo 7, any number in $[4]$ is a multiplicative inverse of 2. Then use this fact to solve the congruence

$$2x \equiv 3 \pmod 7$$

from Checkpoint 4.3.4.

Checkpoint 4.3.7 The Multiplicative Inverse is Unique. Given $a, m \in \mathbb{N}$ such that $\gcd(a, m) = 1$, prove that the multiplicative inverse of a modulo m is unique (up to congruence class).

Hint. Assume that c and d are both multiplicative inverses of a modulo m. Show that $c \equiv d \pmod m$.

Checkpoint 4.3.8 Uniqueness of Solutions. Use the previous exercise to argue that

$$ax \equiv b \pmod m$$

has a unique solution (up to congruence class) if $\gcd(a, m) = 1$.

Does the converse hold? That is, if we know that

$$ax \equiv b \pmod m$$

has a unique solution, can we conclude that $\gcd(a, m) = 1$?

Checkpoint 4.3.9 Solve These Congruences. Solve the congruences:

(a) $5x - 7 \equiv 9 \pmod{11}$

(b) $3 - 2x \equiv 3 - 5x \pmod 7$

(c) $21x + 35 \equiv 9 \pmod{19}$

Checkpoint 4.3.10 How Many Solutions? Since $\gcd(6, 16) > 1$, the number 6 has no multiplicative inverse modulo 16. Solve the congruences

$$6x \equiv 3 \pmod{16}$$

and

$$6x \equiv 4 \pmod{16}.$$

How many solutions do you get for each one (modulo 16)?

4.3.1 ▸▸ Solutions to Selected Checkpoints

4.4▲ Euler's Theorem

Objectives

- Define Euler's totient function $\phi(n)$, compute its values for small n, and prove general statements about $\phi(n)$.
- State and apply Euler's Theorem and Fermat's Little Theorem to solve congruences and prove other results.
- Apply Fermat's Little Theorem to primality testing.

First, let's restate the definition of Euler's totient function (introduced in Exploration 3.2.1).

Definition 4.4.1 Euler's Totient Function.

Euler's totient function (or **Euler's phi-function**) is the function $\phi : \mathbb{N} \to \mathbb{N}$ defined by

$$\phi(m) = \left|\{k \in \mathbb{N} : 1 \leq k \leq m, \gcd(k, m) = 1\}\right|.$$

Example 4.4.2 $\phi(1)$ and $\phi(8)$.

We have $\phi(1) = 1$ since 1 is the only integer in $\{1\}$ relatively prime with 1.

Also $\phi(8) = 4$, since there are four numbers in the set $\{1, 2, \ldots, 8\}$ relatively prime with 8: they are 1, 3, 5, and 7.

Checkpoint 4.4.3 $\phi(n)$ for small n. The table below lists values of $\phi(m)$ for small values of m. Complete the table for $m = 11, 12, \ldots, 20$.

Table 4.4.4

m	integers $1 \leq k \leq m$ such that $\gcd(k, m) = 1$	$\phi(m)$
1	1	1
2	1	1
3	1, 2	2
4	1, 3	2
5	1, 2, 3, 4	4
6	1, 5	2
7	1, 2, 3, 4, 5, 6	6
8	1, 3, 5, 7	4
9	1, 2, 4, 5, 7, 8	6
10	1, 3, 7, 9	4
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		

If p is prime, then by definition all integers from 1 to $p-1$ are relatively prime with p. This implies the following result:

Proposition 4.4.5 $\phi(p)$.

If p is prime, then $\phi(p) = p - 1$.

Checkpoint 4.4.6 **Converse of Proposition 4.4.5.** Is the converse of the above statement true? That is, if $m > 2$ is an integer such that $\phi(m) = m - 1$, does it necessarily follow that m is prime?

Justify your answer.

Checkpoint 4.4.7 $\phi(p^k)$. If p is prime and $k \in \mathbb{N}$, prove that $\phi(p^k) = p^k - p^{k-1}$.

Checkpoint 4.4.8 $\phi(pq)$. If p and q are prime, prove that $\phi(pq) = (p-1)(q-1)$.

Hint. Theorem 3.2.6

Now we can state Euler's Theorem then prove Fermat's Little Theorem, which is a special case.

Theorem 4.4.9 **Euler's Theorem.**

If $a, m \in \mathbb{N}$ with $\gcd(a, m) = 1$, then

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

Theorem 4.4.10 **Fermat's Little Theorem (FLT).**

If $a \in \mathbb{N}$ and p is prime such that $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. If p is prime with $p \nmid a$, we have $\gcd(a, p) = 1$. So we can use Theorem 4.4.9 on a and $m = p$. Since $\phi(p) = p - 1$ by Proposition 4.4.5, the result follows.

Although Theorem 4.4.10 is a special case of Theorem 4.4.9, it was Theorem 4.4.10 that was actually proven first—in 1736, also by Euler [1]. Only in 1763 did Euler publish the generalization that is Euler's Theorem [2].

Example 4.4.11 Example of Theorem 4.4.9.

Take $m = 8$ and $a = 7$ so that $\gcd(a, m) = 1$. By Theorem 4.4.9 we have

$$7^{\phi(8)} \equiv 1 \pmod 8 \Rightarrow 7^4 \equiv 1 \pmod 8.$$

Example 4.4.12 Compute the Remainder.

Compute 3^{2020} **mod** 113.

Solution. Since $\gcd(3, 113) = 1$, we can apply Theorem 4.4.9. In fact, 113 is prime, so Theorem 4.4.10 applies here, so we know that

$$3^{112} \equiv 1 \pmod{13}.$$

Using the Theorem 1.3.2 on 2020 we get $2019 = 18 \cdot 112 + 4$. Hence

$$3^{2020} \equiv (3^{112})^{18} \cdot 3^4 \pmod{113} \equiv 81 \pmod{113}.$$

So 3^{2020} **mod** $113 = 81$.

Checkpoint 4.4.13 Compute the Remainder. Compute 6^{6777} **mod** 667.

Hint. $667 = 23 \times 29$.

The idea behind the proof of Theorem 4.4.9 is that for $a, m \in \mathbb{N}$ relatively prime, multiplying each element of the set

$$S = \{y \in \{1, 2, \ldots, m\} : \gcd(y, m) = 1\}$$

by a induces a permutation of the set modulo m. We give first an example with numbers.

Example 4.4.14 Why Theorem 4.4.9 holds, for $a = 4$ and $m = 9$.

Let $a = 4$ and $m = 9$. Then $\phi(9) = 6$, since the integers $S = \{1, 2, 4, 5, 7, 8\}$ are relatively prime with 9.

Multiplying each number in S by 4 and reducing modulo 9, we have

$$\begin{array}{lcccccc} S = & \{1 & 2 & 4 & 5 & 7 & 8\} & \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \text{(multiply by } a = 4) \\ & 4 & 8 & 16 & 20 & 28 & 32 & \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \text{(reduce modulo 9)} \\ & \{4 & 8 & 7 & 2 & 1 & 5\} & \rightarrow \text{ same as } S! \end{array}$$

What this means is that S and $\{4y : y \in S\}$ contain the same numbers modulo 9; so when we take the product of all elements in these sets, the results must be congruent modulo 9 as well:

$$(4 \cdot 1)(4 \cdot 2)(4 \cdot 4)(4 \cdot 5)(4 \cdot 7)(4 \cdot 8) \equiv (1)(2)(4)(5)(7)(8) \pmod 9.$$

Since each element of S is relatively prime with 9, we can apply

Proposition 4.2.14 to cancel each term, and we are left with

$$(4)(4)(4)(4)(4)(4) \equiv 1 \pmod 9 \Rightarrow 4^{\phi(9)} \equiv 1 \pmod 9$$

since $\phi(9) = 6 = |S|$.

Checkpoint 4.4.15 Repeat the Argument. Replicate the idea in Example 4.4.14 to show that $7^{\phi(15)} \equiv 1 \pmod{15}$.

Finally, we present the proof of Theorem 4.4.9.***Proof of Euler's Theorem***
Let $a, m \in \mathbb{N}$ such that $\gcd(a, m) = 1$.
First define the set

$$S = \{y : 1 \leq y \leq m, \gcd(y, m) = 1\}$$

to be the set of natural numbers smaller than m and relatively prime with m. We know that there are exactly $\phi(m)$ elements in the set S, so we can label them as $S = \{b_1, b_2, \ldots, b_{\phi(m)}\}$, where $\gcd(b_i, m) = 1$ for $i = 1, 2, \ldots, \phi(m)$.

Since we have $\gcd(b_i, m) = 1$ and $\gcd(a, m) = 1$, we must also have

$$\gcd(ab_i, m) = 1 \text{ for any } i = 1, 2, \ldots, \phi(m).$$

We invoke Theorem 1.3.2 now to write ab_i as

$$ab_i = qm + r \text{ for some } 0 \leq r < m,$$

which implies that $ab_i \equiv r \pmod m$.

Combining with the fact that $\gcd(ab_i, m) = 1$, this implies that $\gcd(r, m) = 1$, so r is a natural number smaller than m and relatively prime with m.

In other words, r is in the set S, and we can write $r = b_j$ for some $1 \leq j \leq \phi(m)$. This means for each $1 \leq i \leq \phi(m)$, we have $ab_i \equiv b_j \pmod m$ for some $1 \leq j \leq \phi(m)$.

Furthermore, none of the b_j's are repeated, because no two ab_i terms are equivalent modulo m. (Otherwise, $ab_{i_1} \equiv ab_{i_2} \pmod m \Rightarrow b_{i_1} \equiv b_{i_2} \pmod m$ by Proposition 4.2.14, which is a contradiction as the b_i's are all distinct and smaller than m.)

Hence, each integer ab_i is congruent modulo m to distinct elements in S:

$$\begin{aligned} ab_1 &\equiv b_{j_1} \pmod m \\ ab_2 &\equiv b_{j_2} \pmod m \\ &\vdots \\ ab_{\phi(m)} &\equiv b_{j_{\phi(m)}} \pmod m \end{aligned}$$

Multiplying all the congruences together gives another congruence, where the right-hand-side is just

$$\prod_{k=1}^{\phi(m)} b_{j_k} = \prod_{i=1}^{\phi(m)} b_i$$

since each element of S appears exactly once. Hence,

$$\prod_{i=1}^{\phi(m)} ab_i \equiv \prod_{i=1}^{\phi(m)} b_i \pmod m \Rightarrow a^{\phi(m)} \equiv 1 \pmod m$$

by an application of Proposition 4.2.14.

Exploration 4.4.1 Primality Testing.

Theorem 4.4.10 asserts that ***if*** p is prime and $\gcd(a,p)=1$, ***then*** $a^{p-1}\equiv 1 \pmod{p}$.

(a) Note that the converse of this statement is not true in general: Even if $\gcd(a,m)=1$ and $a^{m-1}\equiv 1 \pmod{m}$, we would not be able to conclude that m is prime.

Can you give examples of pairs a, m such that $\gcd(a,m)=1$ and $a^{m-1}\equiv 1 \pmod{m}$ are both true, but m is not prime.

(b) Complete the contrapositive of Theorem 4.4.10:

If $a, m \in \mathbb{N}$, $\gcd(a,m)=1$, and $a^{m-1}\not\equiv 1 \pmod{m}$, ***then*** _____.

(c) Show that 91 is not prime by using part (b) with $a=2$.

4.5▲ The Chinese Remainder Theorem

Objectives

- State the Chinese Remainder Theorem and use it to solve systems of congruences and related problems.

The Chinese Remainder Theorem is a result in number theory about solving simultaneous systems of several linear congruences. In this section we explore origins and give methods to solve these systems.

Exploration 4.5.1 Sun Zi's Problem.

Sun Zi () was a Chinese mathematician who in his text *Sunzi Suanjing* (3rd to 5th century AD) is said to have written the earliest known reference to systems of linear congruences. In it he writes:

"

—

'A number is repeatedly divided by 3, the remainder is 2; divided by 5, the remainder is 3; and by 7, the remainder is 2. What will the number be?'

—Sun Zi, *Sunzi Suanjing*, Vol. 3, Problem 26 (as cited in [4])

We follow Sun Zi's method of solving this system.

(a) The first condition in Sun Zi's problem can be written as

$$x \equiv 2 \pmod{3}.$$

Write all three conditions as a system of linear congruences.**Answer**.

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

(b) Since the integers 3, 5, and 7 are pairwise relatively prime, then $35^{-1} \pmod 3$ exists. Compute this quantity.

Similarly, compute $21^{-1} \pmod 5$ and $15^{-1} \pmod 7$.

(c) Explain why each of the following congruences hold:

$$\begin{cases} 2 \cdot 35^{-1} \cdot 35 \equiv 2 \pmod 3 \\ 3 \cdot 21^{-1} \cdot 21 \equiv 3 \pmod 5 \\ 2 \cdot 15^{-1} \cdot 15 \equiv 2 \pmod 7 \end{cases}.$$

(d) Explain why we can conclude that

$$x \equiv 2 \cdot 35^{-1} \cdot 35 + 3 \cdot 21^{-1} \cdot 21 + 2 \cdot 15^{-1} \cdot 15 \pmod{105}$$

is a solution to the original system of congruences, and using your answers from (b) simplify this expression to get an answer modulo 105.

Finally, verify that the answer satisfies all three conditions.**Answer**. $x \equiv 233 \equiv 23 \pmod{105}$.

The method outlined in Exploration 4.5.1 actually works for the general case, as long as the moduli in the system are pairwise relatively prime. Before stating our main theorems let's look at a smaller examples, one with only two congruences.

Checkpoint 4.5.1 Two Congruences. Find a natural number x that leaves a remainder of 3 when divided by 5, and a remainder of 1 when divided by 7.

Hint. What are the numbers that satisfy the first condition? Among these, find one satisfying the second as well.

The solution to Checkpoint 4.5.1 did *not* use the same method as Exploration 4.5.1 and instead just relied on listing numbers. This won't be efficient for larger systems, so let's try to proceed more systematically.

Theorem 4.5.2 Solution to a system of two congruences.

Let $m_1, m_2 \in \mathbb{N}$ and $\gcd(m_1, m_2) = 1$, and consider the system

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases}.$$

Perform the following steps:

- *Find the multiplicative inverse of m_2 modulo m_1, call it t.*
- *Find the multiplicative inverse of m_1 modulo m_2, call it s.*

A solution to the given system is

$$x \equiv atm_2 + bsm_1 \pmod{m_1 m_2},$$

and this is unique modulo $M = m_1 m_2$.

Checkpoint 4.5.3 Two Congruences, again. Solve Checkpoint 4.5.1 by writing its two conditions as a system of two congruences and apply the method in Theorem 4.5.2.

Theorem 4.5.2 speaks to the existence and uniqueness of a solution to the given system. Try proving it yourself in the next two exercises!

Checkpoint 4.5.4 Theorem 4.5.2, existence. Prove that $x \equiv atm_2+bsm_1 \pmod{m_1m_2}$ satisfies both congruences in the given system.

Checkpoint 4.5.5 Theorem 4.5.2, uniqueness. Prove that $x \equiv atm_2+bsm_1 \pmod{m_1m_2}$ is the only solution to the given system modulo m_1m_2.

Finally we state a method for a general system of congruences.

Theorem 4.5.6 Solution to a general system of congruences.

Let $m_1, m_2, \ldots, m_n \in \mathbb{N}$ and $\gcd(m_i, m_j) = 1$ for $i \neq j$, and consider the system

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

Perform the following steps:

- *Let $M = m_1m_2\cdots m_n$.*
- *For each $i = 1, 2, \ldots, n$:*
  - *Define $b_i = M/m_i$ (the product of all moduli other than m_i).*
  - *Find the multiplicative inverse of b_i modulo m_i, call it t_i.*

A solution to the given system is

$$x \equiv a_1b_1t_1 + a_2b_2t_2 + \cdots + a_nb_nt_n \pmod{M} \equiv \sum_{i=1}^{n} a_ib_it_i \pmod{M},$$

and this is unique modulo M.

Checkpoint 4.5.7 Sun Zi's System. Verify that the method outlined in Theorem 4.5.6 produces the same steps and answer as in Exploration 4.5.1.

Checkpoint 4.5.8 Practice. Solve the system of congruences

$$\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 5 \pmod{6} \\ x \equiv 6 \pmod{7} \end{cases}$$

using the method in Theorem 4.5.6.

One consequence of Theorem 4.5.6 is that there is a bijection between n-tuples

$$(a_1, a_2, \ldots, a_n) \in \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$$

and congruence classes modulo $M = \prod_{i=1}^{n} m_i$, as long as the moduli m_i are pairwise relatively prime.

That is, any number in $\{0, 1, \ldots, M\}$ has a unique representation as a collection of remainders a_i for each modulus m_i.

Example 4.5.9 From $\mathbb{Z}_{10}$ to $\mathbb{Z}_2 \times \mathbb{Z}_5$.

Let $x \equiv 1 \pmod 2$ and $x \equiv 2 \pmod 5$. Then Theorem 4.5.6 tells us that the solution $x \equiv 7 \pmod{10}$ is unique.

In fact for any pair of remainders modulo 2 and 5, we get a unique congruence class modulo 10 as a solution to the system

$$\begin{cases} x \equiv a_1 \pmod 2 \\ x \equiv a_2 \pmod 5 \end{cases}$$

Verify that we have a bijection between $\mathbb{Z}_2 \times \mathbb{Z}_5$ and $\mathbb{Z}_{10}$:

$\mathbb{Z}_2 \times \mathbb{Z}_5$	$\mathbb{Z}_{10}$	$\mathbb{Z}_2 \times \mathbb{Z}_5$	$\mathbb{Z}_{10}$
$(0,0)$	0	$(1,0)$	5
$(0,1)$	6	$(1,1)$	1
$(0,2)$	2	$(1,2)$	7
$(0,3)$	8	$(1,3)$	3
$(0,4)$	4	$(1,4)$	9

Checkpoint 4.5.10 Computing large powers. Verify that 19 is a solution to the system

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 5 \pmod 7 \end{cases}$$

Then, use this fact to compute 19^{20} **mod** 21.

Hint. Instead of computing large powers of 19, compute large powers of 1 and 5 (with respective moduli) then use Theorem 4.5.2.

4.6▲ Exercises

Additional Exercises for Chapter 4

1. Let
$$R = \{(1,1),(2,2),(1,2),(2,1),(1,3),(3,3),(3,1),(4,4)\}$$
be a relation on the set $\{1,2,3,4\}$. Is R an equivalence relation? Which properties (reflexive, symmetric, transitive) hold/fail?

2. Let S be the set of differentiable functions from $\mathbb{R}$ to $\mathbb{R}$, and let $\star$ be the relation
$$f \star g \Leftrightarrow f'(x) = g'(x).$$
Is $\star$ an equivalence relation? If it is, describe its equivalence classes.

3. Let $\sim$ be the following relation on $\mathbb{Z}$:
$$m \sim n \Leftrightarrow 4 \mid (m^2 - n^2).$$
Is $\sim$ an equivalence relation? If it is, describe its equivalence classes.

4. Let $A_1, A_2, \ldots, A_k$ form a partition of S. Show that the relation
$$R = \{(x,y) : x \text{ and } y \text{ are in the same } A_i\}$$
is an equivalence relation on S.

What are the equivalence classes of R?

5. If R is an equivalence relation on the set S, and $a, b \in S$ such that $a \in [b]$, show that $[a] = [b]$. Do not use Lemma 4.1.9 or Theorem 4.1.10.
6. Compute the remainder when
   (a) 3^{333} is divided by 100
   (b) 5^{444} is divided by 11
   (c) 2^{888} is divided by 8
   (d) 9^{999} is divided by 99
7. Show that $(3 + 3^3 + 3^5 + 3^7 + 3^9 + 3^{11})$ **mod** $10 = 0$.
8. **April 2018 Final.** Without using induction, prove that $11^{n+2} + 12^{2n+1}$ is divisible by 133 for any $n \in \mathbb{N}$.
9. Let N be the product of any k consecutive natural numbers. Prove $k! \mid N$.
10. Find the multiplicative inverse of each integer b modulo m:
    (a) $b = 4, m = 5$
    (b) $b = 13, m = 76$
    (c) $b = 33, m = 7$
    (d) $b = 10, m = 9$
    (e) $b = 100, m = 999$
11. Solve the following congruences. Express your answer as congruence classes of the original modulus.
    (a) $4x \equiv 8 \pmod 5$
    (b) $4x \equiv 3 \pmod 5$
    (c) $2x \equiv 10 \pmod 8$
    (d) $33x + 4 \equiv 2 \pmod 7$
    (e) $100x - 23 \equiv 11 \pmod{99}$
    (f) $31 - 11x \equiv 4x + 8 \pmod{44}$
12. Prove that if $\gcd(a, n) \nmid b$, then $ax \equiv b \pmod n$ has no solutions.
13. Let $a \in \mathbb{N}$ and suppose p is prime. Prove that $a^2 \equiv 1 \pmod p$ if and only if $a \equiv 1 \pmod p$ or $a \equiv -1 \pmod p$.
14. If $m = 2^k$ is a power of 2, explain how you could use repeated squaring to compute a^m **mod** n for any n. Then apply your method to compute 10^{32} **mod** 41.
15. If m is *not* a power of 2, explain how you could use the results of Exercise 4.6.14 to compute a^m **mod** $n$for any n. Then apply your method to compute 17^{26} **mod** 44.

    Hint. Express m as a sum of powers of two.
16. Prove $\phi(p^k q^l) = \left(p^k - p^{k-1}\right)\left(q^l - q^{l-1}\right)$ for primes p and q, and $k, l \in \mathbb{N}$.

    Hint. Checkpoint 4.4.7 and Checkpoint 4.4.8.
17. Find the smallest positive integer y such that
    - y divided by 9 leaves a remainder of 7, and

- y divided by 10 leaves a remainder of 9.

18. Solve the system of congruences

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 2 \pmod 7 \\ x \equiv 1 \pmod{13} \end{cases}$$

using the method outlined in Theorem 4.5.6.

19. Compute each quantity:

(a) 2^{2020} **mod** 5

(b) 2^{2020} **mod** 7

(c) 2^{2020} **mod** 11

(d) 2^{2020} **mod** 385

Hint. $385 = 5 \cdot 7 \cdot 11$.

Chapter 5

Graph Theory

5.1▲ Modeling with Graphs

Objectives

- Something

5.2▲ Definitions and Eulerian Graphs

Objectives

- Something

5.3▲ Isomorphisms and Subgraphs

Objectives

- Something

5.4▲ Connectedness and Trees

Objectives

- Something

5.5▲ Bipartite and Hamiltonian Graphs

Objectives

- Something

5.6▲ Exercises

Additional Exercises for Chapter 5

1.

Appendix A

Notation

Symbol	Description	Page
$A \subseteq B$	set inclusion	??
$\mathbb{N}$	natural numbers	??
$\mathbb{Z}$	integers	??
$\mathbb{Q}$	rational numbers	??
$\mathbb{R}$	real numbers	??
$(a, b), [a, b]$, etc.	intervals of real numbers	??
$f : A \to B$	function	??
$(g \circ f)(x)$	function composition	??
$\lvert A\rvert = \lvert B\rvert$	cardinality, equal	??
$\lvert A\rvert \leq \lvert B\rvert$	cardinality, less than or equal	??
$P(A)$	power set	??
$b \mid a$	divides; divisible by	??
$\gcd(a, b)$	greatest common divisor	??
$n!$	factorial	??
$P(n, k)$, ${}_nP_k$	k-permutation of an n-set	??
$\binom{n}{k}$, $C(n, k)$, ${}_nC_k$	k-combination of an n-set	??
$\lfloor n \rfloor$	floor function	??
D_n	Number of derangements of $\{1, 2, \ldots, n\}$	??
$[x]$	equivalence class of x	??
$a \equiv b \pmod{n}$	congruence modulo n	??
$\mathbb{Z}_n$	Set of congruence classes mod n	??
$a \bmod m$	modulo operation	??
$\phi(n)$	Euler's totient function	??

Appendix B

List of Results

Section 1.1 Sets and Functions

Definition 1.1.1	Set Inclusion and Equality
Definition 1.1.4	Function
Definition 1.1.5	Injective, surjective, bijective
Definition 1.1.7	Composition
Theorem 1.1.8	Properties of Compositions
Definition 1.1.10	Cardinality Relations
Definition 1.1.12	Power Set

Section 1.2 Logic and Proof Techniques

Theorem 1.2.1	Principle of Mathematical Induction

Section 1.3 Integers and Divisibility

Definition 1.3.1	Divisibility and Primes
Theorem 1.3.2	Division Algorithm
Definition 1.3.4	GCD
Theorem 1.3.6	Bezout's Identity
Lemma 1.3.10	Euclid's Lemma

Section 2.1 The Basic Counting Principles

Definition 2.1.6	Partition
Definition 2.1.14	Factorial

Section 2.2 Permutations and Combinations

Definition 2.2.1	Permutation
Proposition 2.2.5	k-permutation of an n-set

(Continued on next page)

(Continued on next page)

Section 4.4 Euler's Theorem

Section 4.5 The Chinese Remainder Theorem

Appendix C

Solutions to Selected Exercises

2 · Counting Techniques

2.7 · Exercises

2.7.4. Solution. b. The rearrangement should start A, I, and I in some order, and end with P, N, and N in some order. These two decisions are independent of each other, so using Principle 2.1.9 and Proposition 2.2.10 we count a total of

$$\frac{3!}{2!} \times \frac{3!}{2!} = 9$$

rearrangements. (Try listing them all!)

2.7.8. Solution. Test

2.7.9. Solution. Hmmmm...

3 · Pigeonhole and Inclusion-Exclusion

3.4 · Exercises

3.4.1. Solution. Define pigeonholes to be $\{1, 2\}$, $\{3, 4\}$, and so on.

References

Euler, L., 1741. Theorematum quorundam ad numeros primos spectantium demonstratio. Euler Archive - All Works by Eneström Number. 54.Euler, L., 1763. Theoremata arithmetica nova methodo demonstrata. Euler Archive - All Works by Eneström Number. 271.Fuchs, S., 2017. MAT102H5 Introduction to Mathematical Proofs. (Course Notes)Kangsheng, S., 1988. Historical development of the Chinese remainder theorem. Arch. Hist. Exact Sci. 38, 285–305.Kolachana, A., Mahesh, K., Ramasubramanian, K., 2019. Use of permutations and combinations in India, in: Kolachana, A., Mahesh, K., Ramasubramanian, K. (Eds.), Studies in Indian Mathematics and Astronomy: Selected Articles of Kripa Shankar Shukla. Springer Singapore, Singapore, pp. 356–376.Wilson, R., Watkins, J.J., 2013. Combinatorics: Ancient & Modern. OUP Oxford.