Math/CS 11 - Discrete Math

Edwin Lin | UCR Summer 2023

Main Text: Schaum's Outline of Discrete Mathematics, Revised 3ed - Lipschutz, Lipson

Additional Texts:

1. A Transition to Advanced Mathematics 7ed,8ed - Andre, Eggen, Smith
2. Discrete Mathematics and Its Applications 7ed - Rosen

Notes on instruction and pacing

These notes were written with the intention of a 5 week Summer session course which meets 4 days per week in 80 minutes sessions. Being a course catered to both CS and math students, there is an attempt to balance important skills for both parties (i.e. induction and combinatorics for CS and proof techniques for math). Of course, the author being a student of mathematics will likely skew this attempt in the obvious direction.

Contents

Introduction

What is discrete math?

Discrete math is a sort of blanket term which covers the introductory material to several fields of mathematics which, in some sense, are devoted to objects which are distinct, finite (or countable), and unconnected to each other:

1. Logic
2. Set theory
3. Number theory

4. Combinatorics
5. Graph theory

which for mathematicians, leads to further study of these topics. For computer scientists, this gives the foundations in order to study topics such as

1. Data structures
2. Algorithms
3. Database theory
4. Automata theory
5. Formal languages
6. Compiler theory
7. Computer security
8. Operating systems

The most important takeaway is the development of your mathematical maturity; the ability to understand and create mathematical arguments even for problems you have not seen before. Finally, it is an ideal environment to learn how to read and write proofs.

Why write proofs?

In a very rough sense, the creation of a theory in the natural and social sciences consists of 4 majors steps

1. Observations, Questions, Data
2. Hypothesis
3. Experimentation
4. Theory

For mathematicians, we follow a similar process, with one major difference

1. Observations, Questions, Data

2. Hypothesis (conjecture)
3. Proof
4. Theory

Proofs are what make mathematics different from all other sciences, because once we have proven something, we are absolutely certain that it is and will always be true. It is not simply a theory that fits our current observations and experiments that could possibly be replaced by a better one in the future.

Why not just test enough examples?

In the natural and social sciences, the truth of a theory relies on experimentation being consistently true under the same circumstances for a finite number of iterations. The difference in mathematics is that the number of iterations required to ascertain truth of a statement is usually infinite.

Take for example the following statement:

$$n^2 - 3n + 43 \text{ is a prime number for any positive integer } n.$$

Testing the first 42 positive integers would lead us to believe this is true, but it turns out

$$(43)^2 - 3(43) + 43 = 1763 = (41)(43) \qquad \text{(not prime)}$$

1 Logic and Proofs

1.1 Propositions and Connectives

Definition 1.1 (Propositions)**.** A **proposition** is a sentence or statement which has a single **truth value**, either true or false. (T/F)

Example 1.2 (4 examples of propositions)**.**

1. Fire is hot. (True)
2. All apples are red. (False)
3. 2 + 2 = 4 (True)
4. 4-3 = 0 (False)

Example 1.3 (4 examples of non-propositions).

1. What is love? (questions aren't statements)
2. Cry for me (commands aren't statements)
3. They live in LA. (depends upon who ”they” refers to)
4. $x^2 = 4$ (depends on the value of ”x”)

Definition 1.4 (Negations). Given a proposition, denoted by P, we call its **negation** to be the proposition which says ”P is false” or ”it is not true that P holds”. We denote the negation of P by $\neg P$.

Example 1.5 (3 simple examples of negations). Let P and R denote propositions.

1. Let P: The lights are off. Then
$$\neg P : \text{ The lights are on.}$$
2. Let R: $2 + 2 = 4$. Then
$$\neg R : \; 2 + 2 \neq 4$$
3. Let Q: $1 < 3$. Then
$$\neg Q : \; 1 \geq 3$$

Remark 1.6. For a proposition P, exactly on of P or $\neg P$ is true. They cannot both be true. Otherwise, we would have a **paradox**.

Definition 1.7 (Compound propositions and logical operators). A **compound proposition** is a statement made up of multiple subpropositions and **logical operators**.

Definition 1.8 (Conjuction). Given propositions P and Q, the **conjunction** of P and Q, denoted $P \wedge Q$ is the proposition ”both P and Q are true”. This is also known as the ”and” proposition.

Definition 1.9 (Disjunction). Given propositions P and Q, the **disjunction** of P and Q, denoted $P \vee Q$ is the proposition ”at least one of P and Q is true”. This is also known as the ”or” proposition.

Example 1.10 (A small example). Let P : The ocean contains water. and $Q : e^{\ln(5)} = 4$.

1. The conjunction $P \wedge Q$ is false since Q is false.
2. The disjunction $P \vee Q$ is true since P is true.

Definition 1.11 (Truth tables). Compound propositions whose truth values depend upon the truth value of several other subpropositions may be expressed by a table organizing all combinations of truth values of subpropositions.

Example 1.12 (Truth tables for conjunction and disjunction)**.**

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Example 1.13 (More complicated example of truth table)**.** Let P, Q, R be propositions

P	Q	R	$\neg R$	$P \wedge Q$	$(P \wedge Q) \vee (\neg R)$
T	T	T	F	T	T
T	T	F	T	T	T
T	F	T	F	F	F
T	F	F	T	F	T
F	T	T	F	F	F
F	T	F	T	F	T
F	F	T	F	F	F
F	F	F	T	F	T

END OF DAY 1

Definition 1.14 (Tautology)**.** A **tautology** is a proposition whose truth value is always true. If a proposition P is a tautology, we say that $P \equiv T$.

Definition 1.15 (Contradiction)**.** A **contradiction** is a proposition whose truth value is always false. If a proposition P is a contradiction, we say that $P \equiv F$.

Example 1.16 (Law of excluded middle)**.**

P	$\neg P$	$P \wedge (\neg P)$
T	F	F
F	T	F

P	$\neg P$	$P \vee (\neg P)$
T	F	T
F	T	T

Hence $P \wedge (\neg P)$ is a contradiction and $P \vee (\neg P)$ is a tautology.

Definition 1.17 (Equivalence of propositions)**.** Two propositions, P, Q are **equivalent** if their truth tables are the same. We denote such equivalence by $P \equiv Q$.

Theorem 1.18 (Transitive property of logical equivalence)**.** Let P, Q, R be propositions such that $P \equiv Q$ and $Q \equiv R$. Then $P \equiv R$.

Theorem 1.19 (Algebra of propositions)**.** For propositions P, Q, R, the following hold:

1. Idempotent laws:
$$P \wedge P \equiv P \qquad \text{and} \qquad P \vee P \equiv P$$

2. Associative laws:
$$(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R) \quad \text{and} \quad (P \vee Q) \vee R \equiv P \vee (Q \vee R)$$

3. Commutative laws:
$$P \wedge Q \equiv Q \wedge P \quad \text{and} \quad P \vee Q \equiv Q \vee P$$

4. Distributive laws:
$$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R) \quad \text{and} \quad P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$$

5. DeMorgan's laws
$$\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q) \quad \text{and} \quad \neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$$

6. Absorption laws
$$P \vee (P \wedge Q) \equiv P \quad \text{and} \quad P \wedge (P \vee Q) \equiv P$$

7. Involution law
$$\neg(\neg P) \equiv P$$

8. Identity law
$$P \vee F \equiv P, \quad P \vee T \equiv T \quad P \wedge F \equiv F, \quad P \wedge T = P$$

Proof.

5.

P	Q	$\neg P$	$\neg Q$	$\neg(P \wedge Q)$	$\neg(P \vee Q)$	$(\neg P) \wedge (\neg Q)$	$(\neg P) \vee (\neg Q)$
T	T	F	F	F	F	F	F
T	F	F	T	T	F	F	T
F	T	T	F	T	F	F	T
F	F	T	T	T	T	T	T

since columns 5 and 8 are the same and columns 6 and 7 are the same, we have that DeMorgan's laws hold.

□

Remark 1.20 (New way to prove $P \equiv Q$)**.** Using the algebra of propositions, we may now prove two propositions are equivalent just from algebraic manipulations instead of directly by definition. (Recall trigonometric identities and their proofs)

Example 1.21 (Using the algebra of propositions)**.** Let P, Q be propositions. Prove that $\neg(P \vee Q) \vee (\neg P \wedge Q) \equiv \neg P$.

Proof.

$$\begin{aligned} \neg(P \vee Q) \vee (\neg P \wedge Q) &= (\neg P \wedge \neg Q) \vee (\neg P \wedge Q) && \text{(DeMorgan's law)} \\ &\equiv \neg P \wedge (\neg Q \vee Q) && \text{(Distributive law)} \\ &\equiv \neg P \wedge T && (\neg Q \vee Q \text{ is a tautology}) \\ &\equiv \neg P && \text{(Identity law)} \end{aligned}$$

□

Definition 1.22 (Conditionals)**.** For propositions P, Q, the **conditional** (or **implication**), denoted $P \implies Q$ is the proposition "if P is true, then Q is true". We call P the **antecedent** (or **assumption**) and Q the **consequence**. The truth table of $P \implies Q$ is given by

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

Example 1.23 (When is the conditional false?)**.** Suppose someone says to a friend, "If it rains, I'll bring an umbrella for you." This promise is broken (i.e. the conditional statement is false) only when rain occurs and the one who made the promise does not bring an umbrella for their friend. This is line 3 of the truth table above. If it doesn't rain at all, we don't say the promise is broken regardless of whether an umbrella is brought or not (lines 2 and 4). Last, the promise is also kept if it does rain and an umbrella is brought (line 1).

Remark 1.24 (Causation)**.** Be careful not to assume that conditional statements are always linked to causation. It could very well be that the assumption and consequence are completely unrelated. Take for example:

$$\text{If } \sin(\pi) = 1, \quad \text{then 6 is prime.}$$

As a conditional proposition, this is true since its assumption is false.

Example 1.25 (Conditional as a disjunction)**.** Prove that $(P \implies Q) \equiv (\neg P \vee Q)$.

Proof. Since we don't yet have any algebraic tools for the conditional proposition, we must prove equivalence from definition, i.e. truth tables.

P	Q	$P \implies Q$	$\neg P \vee Q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

□

Theorem 1.26 (Modus Ponens)**.** Let P, Q be propositions. $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

Another way to phrase this is: if P is true, then $P \wedge (P \implies Q) \equiv Q$.

Definition 1.27 (Converse and contrapositive)**.** The **converse** of $P \implies Q$ is $Q \implies P$. The **contrapositive** of $P \implies Q$ is $\neg Q \implies \neg P$.

Example 1.28 (Equivalence of conditional and contrapositive)**.** From the following truth table

P	Q	$P \implies Q$	$Q \implies P$	$\neg Q \implies \neg P$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

we see that $P \implies Q \equiv \neg Q \implies \neg P$. In other words, the conditional is equivalent to the contrapositive.

Definition 1.29 (Biconditional)**.** For propositions P, Q, the **biconditional** proposition, $P \iff Q$, is the statement ”P if and only if Q.” $P \iff Q$ is true exactly when P and Q have the same truth value. We also abbreviate ”if and only if” by ”iff.”

END OF DAY 2

Example 1.30 (Biconditional as conjunction)**.** Prove that $(P \iff Q) \equiv (P \wedge Q) \vee (\neg P \wedge \neg Q)$

P	Q	$(P \wedge Q) \vee (\neg P \wedge \neg Q)$
T	T	T
T	F	F
F	T	F
F	F	T

Example 1.31 (Biconditional as conjunction of conditionals)**.** Prove that $(P \iff Q) \equiv (P \implies Q) \wedge (Q \implies P)$ using the algebra of propositions.

Proof.

$$\begin{aligned} P \iff Q &\equiv (P \wedge Q) \vee (\neg P \wedge \neg Q) \\ &\equiv [(P \wedge Q) \vee \neg P] \wedge [(P \wedge Q) \vee \neg Q] && \text{(Distributive law)} \\ &\equiv [(P \vee \neg P) \wedge (Q \vee \neg P) \wedge [(P \vee \neg Q) \wedge (Q \vee \neg Q)]] && \text{(Distributive law)} \\ &\equiv [T \wedge (Q \vee \neg P)] \wedge [(P \vee \neg Q) \wedge T] && \text{(Tautologies)} \\ &\equiv (\neg P \vee Q) \wedge (\neg Q \vee P) && \text{(Commutative law)} \\ &\equiv (P \implies Q) \wedge (Q \implies P) \end{aligned}$$

□

Remark 1.32 (Equivalence and biconditionals)**.** Two propositions, P and Q, are equivalent precisely when $P \iff Q$ is a tautology.

1.2 Quantifiers

Definition 1.33 (Quantifiers)**.** The symbol, $\exists$ is the **existential quantifier** and reads "there exists..." or "for some..." The symbol $\forall$ is the **universal quantifier** and reads "for all..." or "for every..."

Remark 1.34 (Negation of quantifiers)**.** Let $P(x)$ be a proposition depending on some variable x.

1. The negation of $\forall x,\ P(x)$ is $\exists x,\ \neg P(x)$.
2. The negation of $\exists x,\ P(x)$ is $\forall x,\ \neg P(x)$.

Example 1.35 (Examples of quantifiers)**.** Consider the collection of all numbers x such that $3 \leq x < 9$. Check the truth value of each statement

1. $P_1 :\ (\forall x),\ (x - 3 > 0)$. False.

$$\neg P_1 : (\exists x), (x - 3 \leq 0)$$

2. $P_2 :\ (\exists x),\ (x - 3 \geq 0)$. True.

$$\neg P_2 : (\forall x),\ (x - 3 < 0)$$

3. $P_3 :\ (\exists x),\ (3 \leq x + 2 < 9)$. True.

$$\neg P_3 : (\forall x), (x + 2 < 3 \vee x + 2 \geq 9)$$

4. $P_4 :\ (\forall x),\ (3 \geq x + 2) \vee (x + 2 > 9)$. False.

$$\neg P_4 : (\exists x),\ (3 < x + 2 \leq 9)$$

5. $P_5: (\forall x), (3 > x+2) \vee (x+2 \geq 9)$. False.

$$\neg P_5 : (\exists x), (3 \leq x+2 < 9)$$

Definition 1.36 ($\exists!$)**.** The symbol $\exists!$ is the **unique existential quantifier** and reads ”there exists a unique...”

1.3 Proof Techniques

Definition 1.37 (Theorem and proof)**.** In mathematics, a **theorem** is a statement that describes a pattern or relationship among quantities and structures. A **proof** is a justification of the truth of a theorem.

Definition 1.38 (Axioms and undefined terms)**.** Similar to other sciences, mathematics cannot begin from nothing, so in any mathematical study, there is an underlying set of **axioms** and **undefined terms** (conceptual atomic particles). These are facts, terms, or quantities that are assumed to be true or known without the need for a proof.

An example of an axiom could be that we'll always assume that $a+b=b+a$ for any two numbers a, b.

An example of an undefined term could be that we all agree we know what a point is when we are solving problems in (Euclidean) geometry.

Remark 1.39 (Basic tools for proofs)**.** When proving a mathematical statement, at any time, you may

1. State an assumption, axiom, or previously proven result (unless otherwise stated).

2. State definitions.

3. State tautologies. For example, if a proof involves a real number x, we can state something like

   We know that $x < 0$ or $x \geq 0$.

4. Utilize modus ponens to chain together implications. For example, we know that if a function f is differentiable on an interval (a, b), then it is continuous on (a, b) as well.

   A proof write who has stated

   f is differentiable on the interval (1,8)

   could then use modus ponens to state

   Therefore, f is continuous on the interval $(1, 8)$.

5. State a proposition which is equivalent to any statement earlier in the proof. For example, if we have the step in a proof which says

   It is not the case that x is even and prime

   then we have a proposition of the form $\neg(P \wedge Q)$ which we know is equivalent to $(\neg P \vee \neg Q)$. Thus, we can immediately state

   x is not even or x is not prime.

END OF DAY 3

1.3.1 Direct Proofs

A **direct proof** of a conditional proposition $P \implies Q$ begins with the assumption that P is true. We then use axioms, definitions, modus ponens, and previously proven theorems to show that Q is true.

Assume P.

$\vdots$

Therefore, Q.

Thus, $P \implies Q$.

Definition 1.40 (Parity)**.** The integer n is **even** if there exists an integer k such that $n = 2k$, and n is **odd** if there exists an integer k such that $n = 2k + 1$.

Example 1.41 (Square parity)**.** Prove that if n is an odd integer, then n^2 is also odd.

Proof. Let n be an odd integer. Then we know by definition 1.40 that there exists an integer k such that $n = 2k + 1$. Squaring both sides, we have

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned}$$

and since $2k^2 + 2k$ is an integer, we see that, by definition of odd numbers, n^2 is odd, completing the proof. □

Example 1.42 (Simple parity proof)**.** Let x, y both be odd integers. Prove that $3x - 5y$ is even.

Proof. Since x, y are odd integers, we know that there exists integers n, m such that $x = 2n+1$ and $y = 2m+1$. Then observe the following

$$\begin{aligned}3x - 5y &= 3(2n+1) - 5(2m+1)\\ &= 6n + 3 - (10m + 5)\\ &= 6n - 10m + 8\\ &= 2(3n - 5m + 4)\end{aligned}$$

Thus, we have shown that $3x - 5y = 2k$ where $k = 3n - 5m + 4$. Hence, $3x - 5y$ is even. □

Example 1.43 (Inequality proof)**.** Let x, y be real numbers. Prove that if $0 \leq x \leq y$, then $x^2 \leq y^2$.

Proof. Since x and y are both nonnegative, we know that $x + y \geq 0$ as well. Moreover, since $y \geq x$, we may subtract x to both side to find $y - x \geq 0$. Thus, taking the product of $y + x$ and $y - x$, we have

$$\begin{aligned}(y+x)(y-x) &\geq 0 && \text{(since both are nonnegative)}\\ y^2 - x^2 &\geq 0 && \text{(difference of squares)}\\ y^2 &\geq x^2\end{aligned}$$

This completes the proof. □

1.3.2 Proof by Exhaustion

A **proof by exhaustion** of a conditional proposition $P \implies Q$ relies on the scenario where P can be expressed as a disjunction of two or more propositions. We'll use two for simplicity.

$$P \equiv P_1 \vee P_2$$

so that

$$(P \implies Q) \equiv [(P_1 \vee P_2) \implies Q] \equiv [(P_1 \implies Q) \wedge (P_2 \implies Q)]$$

The proof then follows the following:

Case 1: Assume P_1
$\vdots$
Therefore Q
Case 2: Assume P_2
$\vdots$
Therefore Q
Thus, in all cases $P \implies Q$.

Example 1.44 (Parity proof)**.** Let a be an integer. Prove that $2a - 1$ is odd.

Proof. We proceed by cases:

1. If a is odd, then $a = 2k + 1$ for some integer k. Thus,

   $$2a - 1 = 2(2k + 1) - 1 = 2(2k) + 2 - 1 = 2(2k) + 1$$

   Since $2k$ is an integer, we see that $2a - 1$ is odd.

2. If a is even, then $a = 2k$ for some integer k. Thus,

   $$2a - 1 = 2(2k) - 1 = 2(2k) - 2 + 2 - 1 = 2(2k - 1) + 1$$

   Since $2k - 1$ is an integer, we see that $2a - 1$ is odd.

Thus, in all cases, we have that $2a - 1$ is odd. □

Example 1.45 (Absolute value proof)**.** Let x be a real number. Prove that $-|x| \leq x \leq |x|$.

Proof. We'll proceed by cases:

1. If $x \geq 0$, then we know $|x| = x$. Thus, we have that $-x \leq x$. Thus, we have

   $$\begin{aligned} -x &\leq x \leq x \\ -|x| &\leq x \leq |x| && \text{(since } x = |x|.\text{)} \end{aligned}$$

2. If $x < 0$, then $|x| = -x$. Thus, $x \leq -x$ Hence we have that

   $$\begin{aligned} x &\leq x \leq -x \\ -(-x) &\leq x \leq -x \\ -|x| &\leq x \leq |x| && \text{(since } -x = |x|.\text{)} \end{aligned}$$

Thus, in all cases, we have $-|x| \leq x \leq |x|$. □

END OF DAY 4

1.3.3 Proof by Contraposition

Example 1.46 (Examples of converses and contrapositives (MOVE BACK LATER))**.** For each of the following propositions, state their converse and contrapositives.

1. If f is differentiable, then f is continuous.

   Converse: If f is continuous, then f is differentiable.
   Contrapositive: If f is not continuous, then f is not differentiable.

2. If $f'(x) = 0$, then x is a critical point of f.

   Converse: If x is a critical point of f, then $f'(x) = 0$.
   Contrapositive: If x is not a critical point of f, then $f'(x) \neq 0$.

3. If x is a real number, then $x \geq 0$ or $x < 0$

   Converse: If $x \geq 0$ or $x < 0$, then x is a real number.
   Contrapositive: If $x < 0$ and $x \geq 0$, then x is not a real number.

4. If $-1 < x < 1$, then $-|x| < x^2 < |x|$.

   Converse: If $-|x| < x^2 < |x|$, then $-1 < x < 1$.
   Contrapositive: If $-|x| \geq x^2$ or $|x| \leq x^2$, then $-1 \geq x$ or $1 \leq x$.

Sometimes, direct proofs will lead to dead ends. One type of indirect proof is known as **proof by contraposition**, or simply the **contrapositive**. Proofs by the contrapositive make use of the fact that the conditional statement is equivalent to its contrapositive

$$(P \implies Q) \iff (\neg Q \implies \neg P)$$

Assume $\neg Q$

$\vdots$

Therefore, $\neg P$

Thus, $\neg Q \implies \neg P$, so by contraposition, $P \implies Q$.

Example 1.47 (Square parity)**.** Let n be an integer. Prove that if n^2 is odd, then n is also odd.

Proof. Let us first try a direct proof. Since n^2 is odd, we know by definition 1.40 there exists an integer k such that $n^2 = 2k + 1$. From here there is not much more we can do and taking the square root doesn't seem to help.

Let us now assume, by the contrapositive, that n is not odd. This means that n must be even, so there exists an integer k such that $n = 2k$. Taking the square on both sides, we see that $n^2 = 2(2k^2)$, hence n^2 is even, i.e., not odd, completing the proof. □

1.3.4 Proof by Contradiction

Suppose we are trying to prove a single proposition P and we begin by assuming $\neg P$ is true. Suppose that we can find a contradiction $(R \wedge \neg R)$, such that $\neg P \implies (R \wedge \neg R)$ is true. Since $(R \wedge \neg R)$ is always false and $\neg P \implies (R \wedge \neg R)$ is true, this must mean that $\neg P$ must also be false, hence P is true.

Assume by contradiction that $\neg P$

$\vdots$

We have a contradiction R and $\neg R$ for some proposition R.

Thus, by contradiction, P must be true.

Definition 1.48 (Rational number)**.** A number r is rational if there exists integers a, b, $b \neq 0$ such that $r = \frac{a}{b}$ where a and b do not share any common factors (i.e. simplified fully).

Example 1.49 (A classic proof)**.** Prove that $\sqrt{2}$ is irrational.

Proof. By contradiction, let us assume that $\sqrt{2}$ is rational. Then by definition 1.48, there exists integers a, b, $b \neq 0$, and a, b sharing no common factors, such that

$$\sqrt{2} = \frac{a}{b}$$

Squaring both sides, we have

$$\begin{aligned} 2 &= \frac{a^2}{b^2} \\ 2b^2 &= a^2 \end{aligned}$$

Thus, a^2 is even. By the contrapositive of example 1.41, we then have that a must also be even. Hence, by definition 1.40, there exists an integer k such that $a = 2k$. Thus returning to our last equation,

$$2b^2 = a^2 = (2k)^2 = 4k^2$$

Dividing by 2 to both ends, we have

$$b^2 = 2k^2$$

Thus, b^2 is even, hence by the contrapositive of example 1.41, b is also even. Thus, by definition 1.40, there exists another integer m such that $b = 2m$. However this means that a and b both share the factor of 2, contradicting our assumption that a, b share no common factors. Therefore, by contradiction, $\sqrt{2}$ must be irrational. □

END OF DAY 5

Remark 1.50 (Contradiction form of proof of $\implies$)**.** When proving an implication $P \implies Q$ by contradiction, we still assume that $(P \implies Q)$ is false, but we note that this occurs only when

$$\text{P is true and Q is false}$$

Thus, we assume P and $\neg Q$ and try to derive a contradiction, but now we have P as a tool we can use.

2 Set Theory

2.1 Basic Concepts of Set Theory

Definition 2.1 (Sets)**.** A **set** is an unordered collection of distinct objects, called elements or members of the set. A set is said to contain its elements. We write $x \in S$ to denote that x is an element of the set S. The notation $x \notin S$ denotes that x is not an element of the set S.

Example 2.2 (Roster method)**.** We may describe sets by writing its roster enclosed by curly brackets:

1. The set V of all letters in the word "hello" is $V = \{$h,e,l,o$\}$.
2. Sets are not bound by datatype. $S = \{2, \text{m}, \text{blue}, \pi\}$ is a valid set (although possibly not meaningful).
3. Sometimes we may use an ellipse, "...", to describe a set without listing all its elements. Let V be the set of all positive integers less than 100, then

$$V = \{1, 2, 3, \ldots, 97, 98, 99\}$$

Remark 2.3 (Important sets)**.** The following are special sets that have near universal notation:

1. $\mathbb{N} = \{0, 1, 2, \ldots\}$ is the set of all **natural numbers**.
2. $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is the set of all integers.
3. $\mathbb{Q} = \{p/q : p \in \mathbb{Z}, q \in \mathbb{Z}, \text{ and } q \neq 0\}$ is the set of all rational numbers.
4. $\mathbb{R}$ is the set of all real numbers.
5. $\mathbb{C}$ is the set of all complex numbers.

Example 2.4 (Set builder (Move Up because of $\mathbb{Q}$ def.))**.** Another way to describe sets is to use set builder notation. The general form is $\{x : x \text{ has some property } P\}$ or $\{x \mid x \text{ has some property } P\}$. We may also sometimes first assign x to an initial set before describing properties.

1. $U = \{n : n \text{ is an odd positive integer less than } 10\}$.
2. $U = \{n \in \mathbb{Z} : 0 < n < 10, n \text{ odd}\}$.

Definition 2.5 (Equality of sets)**.** Two sets are called equal if they have the same elements. In other words, if A, B are sets, then

$$A = B \iff \forall x(x \in A \iff x \in B)$$

Example 2.6 (Simple equal sets)**.**

1. The sets $\{1, 3, 5\}$ is equal to $\{5, 1, 3\}$
2. The sets $\{\mathbb{R}, \mathbb{R}, \mathbb{N}\}$ is equal to $\{\mathbb{R}, \mathbb{N}\}$.

Definition 2.7 (Empty and singleton sets)**.** There is a special set which has no elements, called the **empty set** or **null set**. It is denoted by $\varnothing$ or $\{\}$.

A set with one element is called a **singleton set**.

Remark 2.8 (Be careful with empty set)**.** Note that $\varnothing$ is the empty set, but $\{\varnothing\}$ is a singleton set containing the empty set.

Definition 2.9 (Subset)**.** Let A, B be sets. We say that A is a **subset** of B, and B is a **superset** of A if every element of A is also an element of B. We denote this relation ship by $A \subseteq B$ and $B \supseteq A$. We use the notation $A \nsubseteq B$ to denote that A is not a subset of B.

If we want to stress that A is a strict subset of B, then we only use $A \subset B$ or $B \supset A$.

Theorem 2.10 (Trivial subsets)**.** For every set S, (i) $\varnothing \subseteq S$ and (ii) $S \subseteq S$.

Proof. We will prove (i). Let S be a set. We must show that $\forall x(x \in \varnothing \implies x \in S)$. However since the empty set has no elements, then $x \in \varnothing$ is always false. Thus, the conditional statement $x \in \varnothing \implies x \in S$ is automatically true. Hence $\forall x(x \in \varnothing \implies x \in S)$ holds true. This completes the proof. □

Example 2.11 (Simple example of subsets)**.**

1. $\{1, 3, 5\} \subseteq \{1, 3, 5\}$
2. It is correct to say $\{1, 3, \} \subseteq \{1, 3, 5\}$, but it is more meaningful to say that $\{1, 3, \} \subset \{1, 3, 5\}$

Theorem 2.12 (Subset inclusion)**.** Two set A, B are equal if and only if $A \subseteq B$ and $B \subseteq A$.

Definition 2.13 (Cardinality)**.** Let S be a set. If there are exactly n distinct elements in S where n is a natural number, we say that S is a **finite set** and that n is the **cardinality** of S. We denote the cardinality of S by $|S|$.

If a set is not finite, we say that it is **infinite**.

Example 2.14 (Simple examples of cardinality)**.**

1. Let $S = \{n \in \mathbb{Z} : -3 \leq n < 1\}$, then $|S| = 4$.
2. Let $S = \{n \in \mathbb{N} : n = 3k, \text{ for some } k \in \mathbb{Z}\}$, then S is infinite.

Definition 2.15 (Power set)**.** Let A be a set. The **power set** of A is the set whose elements are the subset of A and is denoted by $\mathscr{P}(A)$. Thus,

$$\mathscr{P}(A) = \{B : B \subseteq A\}$$

END OF DAY 6

Example 2.16 (Examples of power sets)**.** Give the power sets of the following sets:

1. $A_1 = \{1, 2, 3\}$
$$\mathscr{P}(A_1) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$$
2. $A_2 = \varnothing$
$$\mathscr{P}(A_2) = \{\varnothing\}$$
3. $A_3 = \{x, y, z\}$
$$\mathscr{P}(A_3) = \{\varnothing, \{x\}, \{y\}, \{z\}, \{x,y\}, \{x,z\}, \{y,z\}, \{x,y,z\}\}$$
4. $A_4 = \{1, \{6\}, \{1,2,3\}\}$
$$\mathscr{P}(A_3) = \{\varnothing, \{1\}, \{\{6\}\}, \{\{1,2,3\}\}, \{1, \{6\}\}, \{1, \{1,2,3\}\}, \{1, \{6\}, \{1,2,3\}\}\}$$

Theorem 2.17 (Cardinality of $\mathscr{P}$)**.** If A is a set with n elements, then $\mathscr{P}(A)$ is a set with 2^n elements.

Proof. If $n = 0$, that is, if $A = \varnothing$, then $\mathscr{P}(\varnothing) = \{\varnothing\}$, which is a set with $2^0 = 1$ elements. Thus, the theorem is true for the case $n = 0$.

Now suppose A has n elements for $n \geq 1$. We may write $A = \{x_1, x_2, \ldots, x_n\}$. To describe a subset $B \subseteq A$, we need to know for each $x_i \in A$ whether the elements is in B or not. For each x_i, there are two possibilities, either $x_i \in B$ or $x_i \notin B$, so there are

$$\underbrace{2 \cdot 2 \cdot 2 \cdots 2}_{n \text{ many}} = 2^n$$

combinations. □

Theorem 2.18 (Subset inclusion based on power sets)**.** Let A and B be sets. Then $A \subseteq B$ iff $\mathscr{P}(A) \subseteq \mathscr{P}(B)$.

Proof.

($\Rightarrow$) Suppose that $A \subseteq B$. Let $A' \subseteq A$. Then we have that for every $x \in A'$, $x \in A$, and since $A \subseteq B$, we know that $x \in B$. Thus, $A' \subseteq B$, so $A' \in \mathscr{P}(B)$.

($\Leftarrow$) Now suppose that $\mathscr{P}(A) \subseteq \mathscr{P}(B)$. Then for every $A' \subseteq A$, we know $A' \subseteq B$. However, $A \subseteq A$, so $A \subseteq B$.

□

2.2 Set Operations

Definition 2.19 (Union, intersection, difference)**.** Let A, B be sets.

The **union** of A and B is the set $A \cup B = \{x : x \in A \text{ or } x \in B\}$.

The **intersection** of A and B is the set $A \cap B = \{x : x \in A \text{ and } x \in B\}$

The **difference** of A and B is the set $A \setminus B = \{x : x \in A \text{ and } x \notin B\}$.

Definition 2.20 (Disjoint)**.** Two sets A, B are said to be **disjoint** if $A \cap B = \varnothing$.

Example 2.21. Let $A = \{1, 2, 3, 8, 11\}$ and $B = \{1, 3, 5, 7\}$. Then

1. $A \cup B = \{1, 2, 3, 5, 7, 8, 11\}$
2. $A \cap B = \{1, 3\}$.
3. $A \setminus B = \{2, 8, 11\}$
4. $B \setminus A = \{5, 7\}$.
5. $\{4, 5, 6\}$ is disjoint from A
6. $\{4, 5, 6\}$ is not disjoint from B
7. $A \setminus B$ is disjoint from B
8. $B \setminus A$ is disjoint from A.
9. $A \cap B$ is disjoint from both $A \setminus B$ and $B \setminus A$.

Example 2.22. Recall intervals are also sets, i.e., for real numbers a, b, with $a < b$,

$$(a, b) = \{x \in \mathbb{R} : a < x < b\}$$

Consider now the following examples

1. $[3, 6] \cup [4, 8) = [3, 8)$
2. $[3, 6] \cap [4, 8) = [4, 6]$
3. $[3, 6] \setminus [4, 8) = [3, 4)$
4. $[4, 8) \setminus [3, 6] = (6, 8)$
5. $(-\infty, 3) \cup (-12, \infty) = \mathbb{R}$
6. $(-\infty, 3) \cap (-12, \infty) = (-12, 3)$
7. $(-12, \infty) \setminus (-\infty, 3) = [3, \infty)$
8. $(-\infty, 3) \setminus (-12, \infty) = (-\infty, -12]$

Theorem 2.23 (Algebra of sets)**.** For all sets A, B, C,

1. $A \cap \varnothing = \varnothing$, $A \cup \varnothing = A$
2. $A \cup A = A$, $A \cap A = A$
3. $A \cup B = B \cup A$, $A \cap B = B \cap A$ (Commutative)
4. $A \setminus \varnothing = A$
5. $\varnothing \setminus A = \varnothing$
6. $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$ (Associative)
7. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (Distributive)

END OF DAY 7

Proof. We will prove the first distributive property.

($\subseteq$) Let $x \in A \cup (B \cap C)$. Then $x \in A$ or $x \in B \cap C$.

- If $x \in A$, then $x \in A \cup B$ and $x \in (A \cup C)$, so $x \in (A \cup B) \cap (A \cup C)$.
- Otherwise, if $x \in (B \cap C)$, then $x \in B$ and $x \in C$, so $x \in (A \cup B)$ and $x \in (B \cup C)$. Hence $x \in (A \cup B) \cap (A \cup C)$.

($\supseteq$) If $x \in (A \cup B) \cap (A \cup C)$, then $x \in (A \cup B)$ and $x \in (A \cup C)$. Since $x \in (A \cup B)$, we know $x \in A$ or $x \in B$. Similarly, since $x \in (A \cup C)$, we know $x \in A$ or $x \in C$. Let us now consider the following cases:

- If $x \in A$ and $x \in A$, then $x \in A \cup (B \cap C)$.
- If $x \in A$ and $x \in C$, then $x \in A \cup (B \cap C)$.
- If $x \in B$ and $x \in A$, then $x \in A \cup (B \cap C)$.
- If $x \in B$ and $x \in C$, then $x \in (B \cap C)$, so $x \in A \cup (B \cap C)$.

Thus, in all cases, $x \in A \cup (B \cap C)$.

□

Definition 2.24 (Complement)**.** Let U be some **universal set**, which is understood from context to be the ambient setting we are working in. Now, let A be a set such that $A \subseteq U$. Then we define the **complement** of A to be the set $A^c = U \setminus A$.

By convention, we define $U^c = \varnothing$.

Example 2.25. Let $U = \mathbb{N}$

1. If $A = \{0, 1, 2, 3\}$. Then
$$A^c = \{4, 5, 6, \dots\}$$
2. If $E = \{n \in \mathbb{N} : n \text{ is even}\}$, then
$$E^c = \{n \in \mathbb{N} : n \text{ is odd}\}$$

Example 2.26. Let $U = \mathbb{R}$

1. If $A = (1, 5)$. Then
$$A^c = (-\infty, 1] \cup [5, \infty)$$
2. If $B = [19, \infty)$. Then
$$B^c = (-\infty, 19)$$

Theorem 2.27 (Properties of complements)**.** Let U be the universe, and let $A, B \subseteq U$. Then

1. $(A^c)^c = A$.
2. $A \cup A^c = U$.
3. $A \cap A^c = \varnothing$.
4. $A \setminus B = A \cap B^c$.

5. $A \subseteq B$ iff $B^c \subseteq A^c$.

6. DeMorgan's laws:

$$\text{(i) } (A \cup B)^c = A^c \cap B^c \qquad \text{and} \qquad \text{(ii) } (A \cap B)^c = A^c \cup B^c$$

7. $A \cap B = \varnothing$ iff $A \subseteq B^c$.

Proof.

5. ($\Rightarrow$) Suppose that $A \subseteq B$, and let $x \in B^c$. Then $x \notin B$. If we assume that $x \in A$, then since $A \subseteq B$, then $x \in B$, which contradicts $x \notin B$. Thus, $x \notin A$, so $x \in A^c$. Hence $B^c \subseteq A^c$.

   ($\Leftarrow$) Suppose that $B^c \subseteq A^c$ and let $x \in A$. If $x \in B^c$, then since $B^c \subseteq A^c$, we have that $x \in A^c$, which contradicts $x \in A$. Thus, $x \notin B^c$, so $x \in (B^c)^c = B$. Hence $A \subseteq B$.

6.i

$$\begin{aligned} x \in (A \cup B)^c &\iff x \notin (A \cup B) \\ &\iff \neg(x \in A \vee x \in B) \\ &\iff \neg(x \in A) \wedge \neg(x \in B) \\ &\iff x \notin A \wedge x \notin B \\ &\iff x \in (A^c \cap B^c) \end{aligned}$$

□

Definition 2.28 (Ordered pairs and n-tuples)**.** The **ordered pair** formed from two objects a and b is the object (a, b). Two ordered pairs $(a, b), (c, d)$ are considered **equal** if $a = c$ and $b = d$ and we write $(a, b) = (c, d)$.

We also say that **ordered n-tuples** $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ are equal if $a_i = b_i$ for $i = 1, 2, \ldots, n$.

Definition 2.29 (Cartesian product)**.** Let A, B be sets. The **product** (or **cross product** or **Cartesian product**) of A and B is the set

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

We read $A \times B$ as "A cross B".

Example 2.30 (Simple Cartesian product)**.** If $A = \{a, b\}$ and $B = \{1, 3, 5\}$, then

$$A \times B = \{(a, 1), (a, 3), (a, 5), (b, 1), (b, 3), (b, 5)\}$$

$$B \times A = \{(1, a), (3, a), (5, a), (1, b), (3, b), (5, b)\}$$

since order matters, we immediately see that $A \times B \neq B \times A$ does not hold in general.

Theorem 2.31 (Properties of products)**.** If A, B, C, D are sets, then

1. $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
2. $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
3. $A \times \varnothing = \varnothing$.
4. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.
5. $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.
6. $(A \times B) \cap (B \times A) = (A \cap B) \times (A \cap B)$.

2.3 Mathematical Induction

Remark 2.32 (Intuition behind mathematical induction)**.** Suppose we have an infinite staircase, and we want to convince a friend we can reach every step of the stairs. Our strategy invovles two steps.

1. Prove I can get on the first step.
2. Prove that if I'm on any particular step, then I can take another step up.

By (1), we know we can reach the first step. By (2), since we're on the first step, we can take another to reach the second step. Repeating (2) over and over, we can reach the 3rd, 4th, 5th step and so on.

Definition 2.33 (Principle of mathematical induction)**.** To prove a statement $(\forall n \in \mathbb{N})$, $(P(n))$, we complete two steps:

1. (**Basis step**) We verify that $P(0)$ is true.
2. (**Inductive step**) We show that the conditional statement $P(k) \implies P(k+1)$ for an arbitrary $k \in \mathbb{N}$.

The assumption that $P(k)$ is true is somtimes refered to as the **inductive hypothesis**.

END OF DAY 8

Example 2.34 (Sum of first n naturals)**.** Show that if n is a positive integer, then

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

Proof. We proceed by induction: Let $P(n)$ be the proposition that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

(Basis step) For $n = 1$. We see that

$$1 = \frac{1(1+1)}{2} = \frac{2}{2} = 1$$

holds. Thus, the basis step is complete.

(Inductive step) Assume that $P(k)$ holds true for an arbitrary positive integer k. That is, we assume

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

For the $k+1$ case, we see that

$$\begin{aligned} 1 + 2 + \cdots + k + (k+1) &= (1 + 2 + \cdots + k) + (k+1) && \text{(regrouping)} \\ &= \frac{k(k+1)}{2} + (k+1) && \text{(inductive hypothesis)} \\ &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

The last equation shows that $P(k+1)$ is true under the assumption that $P(k)$ is true. This completes the inductive step.

Since the basis and inductive steps are complete, by mathematical induction, we know that $P(n)$ is true for all positive integers n. □

Example 2.35 (Sum of odds)**.** Find a formula for the sum of the first n positive odd integers. Then prove the formula using mathematical induction.

$$\begin{aligned} 1 &= 1 \\ 1 + 3 &= 4 = 2^2 \\ 1 + 3 + 5 &= 9 = 3^2 \\ 1 + 3 + 5 + 7 &= 16 = 4^2 \\ 1 + 3 + 5 + 7 + 9 &= 25 = 5^2 \\ &\vdots \\ 1 + 3 + 5 + 7 + 9 + \cdots + (2n-1) &= n^2 \end{aligned}$$

Proof. We proceed by induction: Let $P(n)$ be the proposition that $1 + 3 + \cdots + (2n-1) = n^2$.

(Basis step) Let $n = 1$. We see that $1 = 1^2$ holds, completing the basis step.

(Inductive step) Assume that $P(k)$ holds true for an arbitrary positive integer k. That is, we assume

$$1 + 3 + \cdots + (2k - 1) = k^2$$

For the $k + 1$ case, we see that

$$\begin{aligned} 1 + 3 + \cdots + (2k-1) + (2k+1) &= (1 + 3 + \cdots + (2k-1)) + (2k+1) \\ &= k^2 + 2k + 1 && \text{(inductive hypothesis)} \\ &= (k+1)^2 && \text{(factoring)} \end{aligned}$$

The last equation shows that $P(k + 1)$ is true under the assumption that $P(k)$ is true. This completes the inductive step.

Thus, by the principle of mathematical induction, $P(n)$ is true for all positive integers n. □

Example 2.36 (Exponential factorial inequality)**.** Prove, for all integers greater than 3, $2^n < n!$.

Proof. We proceed by induction: Let $P(n)$ be the proposition that $2^n < n!$.

(Basis step) Let $n = 4$. We see that $2^4 = 16 < 4! = 24$.

(Inductive step) Assume that $P(k)$ holds true for an arbitrary positive integer $k > 3$. That is, we assume

$$2^k < k!$$

For the $k + 1$ case, we see that

$$\begin{aligned} 2^{k+1} &= 2(2^k) \\ &< 2(k!) && \text{(inductive hypothesis)} \\ &< (k+1)k! && \text{(since } k > 3\text{)} \\ &= (k+1)! \end{aligned}$$

This completes the inductive step.

Thus, by the principle of mathematical induction $P(n)$ is true for all integers $n > 3$. □

3 Introduction to Combinatorics

3.1 Basic Counting Principles

Theorem 3.1 (Product rule)**.** If A and B are finite sets, then $|A \times B| = |A| \cdot |B|$.

Corollary 3.1.1 (Generalized product rule)**.** If $A_1, A_2, \ldots, A_n$ are sets, then

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_n|$$

Remark 3.2 (How to use the product rule)**. The product rule**: Suppose that a procedure can be broken down into a sequence of two tasks. If there are $n_1 \in \mathbb{N}$ ways to do the first task, and for each of these ways of doing the first task, there are $n_2 \in \mathbb{N}$ ways to do the second task, then there are $n_1 n_2$ ways to do the procedure.

We may generalize this for a procedure which may be broken down into a sequence of m many tasks. If $n_1, n_2, \ldots, n_m$ represent the number of ways to do each respective tasks, then there are

$$n_1 n_2 \cdots n_m$$

ways to do the procedure.

Example 3.3 (Chairs with two labels)**.** The chairs of an auditorium are to be labeled with an uppercase English letter followed by a positive integer in the set $\{1, 2, \ldots, 100\}$. What is the largest number of chairs that can be labeled differently?

Solution: The procedure of labeling chairs consists of two tasks: (1) Assigning a letter, of which there are 26 in the English alphabet, followed by (2) assigning a number from the set $\{1, \ldots, 100\}$ of which there are 100 numbers. Thus, the total number of distinctly labeled chairs is

$$\boxed{26 \cdot 100 = 2600}$$

Example 3.4 (Bit strings)**.** How many different bit strings of length 9 are there?

Solution: A **bit** is short for a **binary digit** which is the most basic unit of information in a digital device. It takes on the value of either 0 or 1. We may assign one of these values for each bit in a string of 9 bits. Thus, there are

$$\boxed{2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^9 = 512}$$

possible distinct bit strings of length 9.

In general, for a bit string of length N, there are 2^N possible strings.

END OF DAY 9

Theorem 3.5 (Sum rule)**.** If A, B are disjoint sets, then

$$|A \cup B| = |A| + |B|$$

Corollary 3.5.1 (Generalized sum rule)**.** If $A_1, A_2, \ldots, A_n$ are pairwise disjoint sets, then

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{i=1}^{n} |A_i|$$

Remark 3.6 (How to use sum rule)**. The sum rule**: If a procedure can be done either in one of n_1 ways or one of n_2 ways where none of the set of n_1 ways is the same as any of the set of n_2 ways, then there are $n_1 + n_2$ ways to do the procedure.

We may generalize this to a procedure which can be done in either $n_1, n_2, \ldots, n_m$ many ways where no two ways are the same. Then there are $n_1 + n_2 + \cdots + n_m$ many ways to do the procedure.

Example 3.7 (Math faculty or math student)**.** Suppose a university would like to select either a math faculty or a student who is majoring in math to be the representative at a local conference. If there are 8 math faculty and 58 math students, how many different choices are there?

Solution: Since one cannot be both a math faculty and a math student, then there are simply $\boxed{8 + 58 = 66}$ possible choices.

Example 3.8 (Code block)**.** What is the value of k after executing the following code?

```
k := 0
for i_1 := 1 to n_1
    k := k+1
for i_2 := 1 to n_2
    k := k+2
for i_3 := 1 to n_3
    k := k+3
```

Solution: Since k starts at 0 and each loop is independent from each other, we simply need to count how many iterations each loop undergoes and how big their increment is.

1. Loop 1 has n_1 many iterations of increments of 1, so we add n_1 to k
2. Loop 2 has n_2 many iterations of increments of 2, so we add $2n_2$ to k
3. Loop 3 has n_3 many iterations of increments of 3, so we add $3n_3$ to k

Thus, in total, k will end with value

$$\boxed{n_1 + 2n_2 + 3n_3}$$

Theorem 3.9 (Principle of inclusion-exclusion)**.** Let A, B be sets. Then

$$|A \cup B| = |A| + |B| - |A \cap B|$$

This is sometimes referred to as the **subtraction rule**.

Proof. Observe that $A = (A \setminus B) \cup (A \cap B)$ and $B = (B \setminus A) \cup (A \cap B)$ where $(A \cap B), (A \setminus B), (B \setminus A)$ are all pairwise disjoint. Using the sum rule, we see that

$$|A| = |A \setminus B| + |A \cap B| \qquad \text{and} \qquad |B| = |B \setminus A| + |A \cap B|$$

Taking their sum, we have

$$\begin{aligned} |A| + |B| &= |A \setminus B| + |A \cap B| + |B \setminus A| + |A \cap B| \\ |A| + |B| - |A \cap B| &= |A \setminus B| + |A \cap B| + |B \setminus A| \\ &= |(A \setminus B) \cup (A \cap B) \cup (B \setminus A)| \qquad \text{(pairwise disjoint + sum rule)} \\ &= |A \cup B| \end{aligned}$$

□

Example 3.10 (Company hires)**.** A tech company receives 750 applications from college graduates. Suppose that 519 majored in computer science, 306 majored in computer engineering, and 76 majored in both computer science and computer engineering. How many of these applicants majored in neither of the two disciplines?

Solution: Let CS be the set of students who majored in computer science and CE be the set of students who majored in computer engineering. Our goal is to find $|(CS \cup CE)^c|$. We define U to be the set of all applicants.

$$\begin{aligned} |(CS \cup CE)^c| &= |U| - |CS \cup CE| \\ &= |U| - (|CS| + |CE| - |CS \cap CE|) \qquad \text{(inclusion-exclusion)} \\ &= 750 - (519 + 306 - 76) \\ &= 1 \end{aligned}$$

Example 3.11 (Bit strings)**.** How many bit strings of length 11 either start with the two bit 11 or end with a 0 bit?

Solution: There are 3 scenarios we must consider that satisfy our requirement

1. A string which only starts with the two bit 11:

$$1\,1\,\underbrace{x_3\,x_4\,x_5\,x_6\,x_7\,x_8\,x_9\,x_{10}\,x_{11}}_{\text{9 bits to assign}}$$

   of which there are $2^9 = 512$ possible strings.

2. A string which only ends in a 0 bit:

$$\underbrace{x_1\,x_2\,x_3\,x_4\,x_5\,x_6\,x_7\,x_8\,x_9\,x_{10}}_{\text{10 bits to assign}}\,0$$

   of which there are $2^{10} = 1024$ possible strings

3. A string with both of the above properties:

$$1\,1\,\underbrace{x_3\,x_4\,x_5\,x_6\,x_7\,x_8\,x_9\,x_{10}}_{\text{8 bits to assign}}\,0$$

of which there are $2^8 = 256$ possible strings.

Thus, in total, we have

$$2^9 + 2^{10} - 2^8 = 512 + 1024 - 256 = \boxed{1280} \text{ possible strings.}$$

Example 3.12 (string of letters)**.** How many lowercase strings of length 4 contain the letter x?

Solution: Let us define X_1, X_2, X_3, X_4 to be the sets which contain 1,2,3, and 4 x's respectively. It is clear that

$$X_4 \subset X_3 \subset X_2 \subset X_1$$

but the total number of lowercase strings of length 4 should be given by

$$|X_1 \cup X_2 \cup X_3 \cup X_4|$$

However instead of calculating this directly, we may use

$$|X_1 \cup X_2 \cup X_3 \cup X_4| = |U| - |(X_1 \cup X_2 \cup X_3 \cup X_4)^c|$$

Thus, there are

$$\boxed{26^4 - 25^4} \text{ lower case strings of length 4 that contain x.}$$

END OF DAY 10

Definition 3.13 (Permutation)**.** Let $A = \{x_1, x_2, \ldots, x_n\}$, i.e., a set of n elements. A **permutation** of A is an ordered arrangement of the elements of the set in a specific order. For $k \in \mathbb{N}$ $1 \leq k \leq n$, a $k-$permutation of A is an ordered arrangement of k elements of A.

Example 3.14. Let $A = \{a, b, c\}$. Then the permutations of A are the following:

$$\begin{array}{cc} abc & acb \\ bac & bca \\ cab & cba \end{array}$$

These are also known as the 3-permutations of A. The 2-permutations of A are

$$ab \quad ba \quad ac \quad ca \quad bc \quad cb$$

The 1-permutations of A are

$$a \quad b \quad c$$

Theorem 3.15 (Number of permutations)**.** The number of k-permutations of a set with n elements is given by

$$P(n,k) = n(n-1)\cdots(n-k+1)$$

Proof. We will use the product rule to prove that this formula is correct (you may also use induction). The first element of the permutation can be chosen in n ways since there are n many elements in the set to begin with. After this, there are $n-1$ elements to choose from for the second position. Continuing this process, there are $n-(r-1) = n-r+1$ ways to choose the rth element Consequently, by the product rule, there are

$$n(n-1)\cdots(n-r+1) \quad r\text{-permutations of the set.}$$

□

Corollary 3.15.1. If $n, r \in \mathbb{N}$ with $r \leq n$, then $P(n,r) = \frac{n!}{(n-r)!}$.

Example 3.16. How many permutations of the letters $ABCDEFGHIJK$ contain the string ACE.

Solution: Since the letters ACE must occur as a block, and there are 8 letters remaining, $BDFGHIJK$, of which there are

$$P(8,8) = \frac{8!}{0!} = \frac{8!}{1} = 8! \text{ permutations.}$$

but since ACE can be placed between any two letters or on either of the outer edges, we have $\boxed{9!}$ permutations of $ABCDEFGHIJK$ in which ACE occurs.

Example 3.17. How many committees of three students can be formed from a group of four students?

Solution: Let us denote the four students by A, B, C, D. Different from the previous problem, if we count permutations, then

$$ABC \qquad \text{and} \qquad ACB$$

would appear as different 3-permutations, but we know that the collection of students A, B, C and A, C, B is the exact same collection of students. Thus, order here does not matter.

Hence, we just need to count the number of subsets of $\{A, B, C, D\}$ which have cardinality 3. That is,

$$\{A, B, C\}, \{A, B, D\}, \{A, C, D\}, \{B, C, D\}$$

i.e., $\boxed{4}$ choices.

Definition 3.18 (Combinations)**.** Let $A = \{x_1, x_2, \ldots, x_n\}$, i.e., a set of n elements and let $k \in \mathbb{N}$ with $k \leq n$. A k**-combination** of A is an unordered selection of k elements from the set A. Thus, a k-combination is simply of subset of A that has k elements.

Example 3.19. Let $A = \{a, b, c, d\}$ then the possible 2-combinations are

$$\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}$$

Hence, there are 6 in total.

Theorem 3.20 (Number of combinations)**.** The number of k-combinations of a set of n elements, where $n, k \in \mathbb{N}$ with $k \leq n$, equals

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

Proof. The $P(n, k)$ k-permutations of the set can be ordered by first forming the $C(n, k)$ k-combinations of the set, and then considering all possible orderings of each set. This is given by $P(k, k)$. Hence,

$$\begin{aligned} P(n, k) &= C(n, k) \cdot P(k, k) \\ C(n, k) &= \frac{P(n, k)}{P(k, k)} \\ C(n, k) &= \frac{\frac{n!}{(n-k)!}}{\frac{k!}{0!}} \\ &= \frac{n!}{k!(n-k)!} \end{aligned}$$

□

Definition 3.21 (Binomial coefficient)**.** $C(n, k)$ is also denoted by the symbol $\binom{n}{k}$ which is known as the **binomial coefficient**. $\binom{n}{k}$ is often read as "n choose k".

Example 3.22 (Card counting)**.** Consider a standard deck of 52 playing cards.

(a) How many hands of 5 cards can be dealt?

(b) How many ways are there to choose 47 cards?

Solution:

(a) Since the order in which the 5 cards are dealt doesn't matter, we see that we are trying to "choose 5 from 52". Thus, there are

$$C(52, 5) = \frac{52!}{5!47!} = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48 \cdot 47 \cdot 46 \cdots 1}{5! \cdot 47 \cdot 46 \cdots 1} = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5 \cdot 4 \cdot 3 \cdot 2} = 2,598,960$$

different hands of 5 cards that can be dealt.

(b) As the question is written, we are trying to "choose 47 from 52". Hence there are

$$C(52,47) = \frac{52!}{47! \cdot 5!} = \boxed{2,598,960}$$

possible ways.

Thus, we see that $C(52,5) = C(52,47)$.

Corollary 3.22.1. Let $n, k \in \mathbb{N}$ with $k \leq n$. Then $C(n,k) = C(n,n-k)$.

Example 3.23. How many subsets containing an even number of elements does a set with 10 elements contain.

Solution: Since the set has 10 elements, we are looking to count the number of subsets that contain either 0,2,4,6,8, or 10 elements. Since sets are unordered, we see that the total number of even cardinality subsets is given by

$$\begin{aligned}
&C(10,0) + C(10,2) + C(10,4) + C(10,6) + C(10,8) + C(10,10)\\
&\qquad = 2C(10,0) + 2C(10,2) + 2C(10,4)\\
&\qquad = 2\frac{10!}{10!0!} + 2\frac{10!}{8!2!} + 2\frac{10!}{6!4!}\\
&\qquad = 2 + 2\frac{10 \cdot 9}{2} + 2\frac{10 \cdot 9 \cdot 8 \cdot 7}{4 \cdot 3 \cdot 2}\\
&\qquad = 2 + 90 + 20 \cdot 3 \cdot 7\\
&\qquad = \boxed{512}
\end{aligned}$$

Example 3.24. Suppose there are 9 math faculty and 13 CS faculty. How many ways are there to select a joint committee if it must contain exactly 4 math faculty and 6 CS faculty?

Solution: We can break this down into two tasks: first looking at the ways we can choose 4 math faculty, then for each of these ways, we can choose 6 CS faculty. Using the product rule, the answer is then the product of 4-combinations from a set of 9 math faculty and 6-combinations from a set of 13 CS faculty. Thus, we have

$$C(9,4) \cdot C(13,6) = \frac{9!}{4!5!} \cdot \frac{13!}{6!7!} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{4 \cdot 3 \cdot 2} \cdot \frac{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2} = \boxed{216,216}$$

Example 3.25. How many bit strings of length 7 are there if the number of 1s is strictly greater than the number of 0s.

Solution: We first observe that if there are more 1s than 0s, the only possible configurations are

1. 7 1s and 0 0s
2. 6 1s and 1 0s

3. 5 1s and 2 0s

4. 4 1s and 3 0s

Thus, if we can find the number of arrangements in each, then we just need to add them all.

Next, take for example, the configuration of 5 1s and 2 0s. If we first place the 2 0s,

$$x_1\,0\,x_3\,x_4\,0\,x_6\,x_7$$

then it is clear that 1s will fill the remaining positions. Thus, arranging the 2 0s is the same as arranging the 5 1s. Hence if we find all possible ways to arrange the 2 0s, it also gives us all possible ways to arrange the 5 1s. Hence, we are ”choosing 2 positions from 7 spots”.

Using this idea, we see that the total number of strings that have more 1s than 0s is given by

$$C(7,0)+C(7,1)+C(7,2)+C(7,3)=\frac{7!}{0!7!}+\frac{7!}{1!6!}+\frac{7!}{2!5!}+\frac{7!}{3!4!}=1+7+21+35=\boxed{64}$$

Another way to solve this problem is to note that the role of 0 and 1 is arbitrary, so the number of strings with more 1s than 0s is exactly the same as the number of strings with more 0s than 1s. There is no scenario where the number of 0s and 1s are equal since we have an odd length string. In total there are 2^7 possible length 7 bit strings, so we simply cut that number in half to get

$$\frac{2^7}{2}=2^6=\boxed{64}$$

END OF DAY 11

4 Introduction to Number Theory

4.1 Divisibility and Modular arithmetic

Definition 4.1 (Divisibility)**.** If $a, b \in \mathbb{Z}$ with $a \neq 0$, we say that a **divides** b if there exists an integer c such that $b = ac$ (or equivalently, if $\frac{b}{a} \in \mathbb{Z}$). When a divides b, we say that a is a **factor** or **divisor** of b and that b is a **multiple** of a. The notation $a \mid b$ denotes that a divides b. We write $a \nmid b$ when a does not divide b.

Example 4.2 (Basic examples)**.** Determine whether $3 \mid 7$ and $3 \mid 12$.

Solution: We see that $3 \nmid 7$ since $\frac{7}{3} \notin \mathbb{Z}$ and $3 \mid 12$ since $\frac{12}{3} = 4 \in \mathbb{Z}$.

Example 4.3 (Number of multiples)**.** Let n, d be positive integers. How many positive integers not exceeding n are divisible by d.

Solution: The positive integers divisible by d are all in the form kd where k is a positive integer. Hence the number of positive integers divisible by d that do not exceed n is the same as the number of k such that

$$\begin{gathered} 0 < kd \leq n \\ 0 < k \leq \frac{n}{d} \end{gathered}$$

However, if $d \nmid n$, then we may only go up to the greatest integer which does not exceed $\frac{n}{d}$, i.e. $\lfloor \frac{n}{d} \rfloor$. Therefore there are $\lfloor \frac{n}{d} \rfloor$ positive integers not exceeding n which are divisible by d.

Theorem 4.4 (Basic properties of divisibility)**.** Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. Then

(i) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$

(ii) if $a \mid b$, then $a \mid bc$ for all $c \in \mathbb{Z}$

(iii) if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. We will prove (i). By definition, if $a \mid b$ and $a \mid c$, then there exists $m, n \in \mathbb{Z}$ such that

$$b = ma \qquad \text{and} \qquad c = na$$

Thus,

$$b + c = ma + na = (m + n)a$$

and since $m + n \in \mathbb{Z}$, we have that $a \mid (b + c)$. □

Corollary 4.4.1. If $a, b, c \in \mathbb{Z}$ with $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ whenever $m, n \in \mathbb{Z}$.

Proof. Since $a \mid b$ and $a \mid c$, we know by (ii), that $a \mid mb$ and $a \mid nc$ for any integers m, n. Then by (i), we know that $a \mid (mb + nc)$. □

Theorem 4.5 (The division algorithm)**.** Let $a \in \mathbb{Z}$ and d be a positive integer. Then there are unique integers q and r with $0 \leq r < d$, such that $a = qd + r$.

Definition 4.6 (Remainder)**.** In the equality $a = qd + r$ from the division algorithm d is called the divisor, a is called the dividend, q is called the **quotient** and r is called the **remainder**. The notation used to denote quotient and remainder are

$$q = a \,\mathbf{div}\, d, \qquad r = a \,\mathbf{mod}\, d$$

Example 4.7 (Basic example)**.** What are the quotient and remainder when 101 is divided by 11?

Solution: We see that

$$101 = 9(11) + 2$$

Hence the quotient is $9 = 101 \,\mathbf{div}\, 11$ The remainder is $2 = 101 \,\mathbf{mod}\, 11$.

Definition 4.8 (Modulo operator)**.** If $a, b \in \mathbb{Z}$ and m is a positive integer then a is **congruent** to b **modulo** m is m divides $a - b$. We use the notation

$$a \equiv b \pmod{m}$$

to indicate that a is congruent to b modulo m.

END OF DAY 12

Theorem 4.9. *Let $a, b \in \mathbb{Z}$ with m being a positive integer. Then $a \equiv b \pmod{m}$ iff there is an integer k such that $a = b + km$.*

Proof.

$$\begin{aligned} a \equiv b \pmod{m} &\iff m \mid (a - b) \\ &\iff a - b = km && \text{(for some } k \in \mathbb{Z}) \\ &\iff a = b + km \end{aligned}$$

□

Theorem 4.10. *Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then*

$$a + c \equiv (b + d) \pmod{n} \qquad \text{and} \qquad ac = bd \pmod{m}.$$

Proof. Since $a \equiv b \pmod{m}$, by theorem 4.9, there are integers s and t, such that $b = a+sm$ and $d = c + sm$. Hence

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$$

and

$$bd = (a + sm)(a + tm) = ac + m(at + cs + stm)$$

Hence $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$. □

Definition 4.11 (Arithmetic modulo m)**.** Let m be a positive integer and define $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$. We now define two new operations on the numbers in this set: **addition modulo** m and **multiplication modulo** m, denoted $+_m$ and $\cdot_m$ respectively. These are defined as

$$\begin{aligned} a +_m b &= (a + b) \mod m \\ a \cdot_m b &= (a \cdot b) \mod m \end{aligned}$$

When using the two operations, we are said to be doing **arithmetic modulo** m.

Example 4.12 (Addition modulo 12)**.** Using the definition of arithmetic modulo 12, see that

$$\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

and

$$\begin{aligned} 7 +_{12} 10 &= (7 + 10) \mod 12 = 17 \mod 12 = 5 \\ 7 \cdot_{12} 10 &= (7 \cdot 10) \mod 12 = 70 \mod 12 = 10 \end{aligned}$$

Theorem 4.13 (Properties of $+_m$ and $\cdot_m$)**.** Let $a, b, c \in \mathbb{Z}_m$.

1. (Closure) $a +_m b$ and $a \cdot_m b$ belong to $\mathbb{Z}_m$
2. (Associativity) $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
3. (Commutativity) $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
4. (Identity) The elements $0, 1$ are identity elements for addition and multiplication modulo m respectively. That is, if a
5. (Additive inverse) If $a \neq 0$, then $m - a$ is an additive inverse of a modulo m and 0 is its own inverse. That is, $a +_m (m - a) = 0$ and $0 +_m 0 = 0$.
6. (Distributivity) $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$

Remark 4.14 ($\mathbb{Z}_m$ is a commutative ring)**.** Under the properties of theorem 4.13, we have that $(\mathbb{Z}_m, +_m, \cdot_m)$ forms a type of structure called a **commutative ring** or **Abelian ring**. If we exclude multiplication modulo m, then $(\mathbb{Z}_m, +_m)$ forms a structure called a **commutative/Abelian group**. Groups and rings are studied in abstract algebra.

END OF DAY 13

4.2 Prime numbers and GCD

Definition 4.15 (Prime number)**.** An integer $p > 1$ is called **prime** if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called **composite**.

Theorem 4.16 (The fundamental theorem of arithmetic)**.** Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes, where the prime factors are written in nondecreasing order.

Example 4.17 (Prime factorization)**.** Find the prime factorization of 76.

$$76 = 2 \cdot 38 = 2 \cdot 2 \cdot 17 = 2^2 \cdot 17$$

Find the prime factorization of 396.

$$396 = 3 \cdot 132 = 3 \cdot 2 \cdot 66 = 3 \cdot 2 \cdot 2 \cdot 3 \cdot 11 = 2^2 \cdot 3^2 \cdot 11$$

Theorem 4.18 (Size of prime factor)**.** If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Proof. If n is composite, by definition, we know it has a factor a with $1 < a < n$. Hence we know that $n = ab$ where b is a positive integer greater than 1. We will show that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

By contradiction, if $a > \sqrt{n}$ and $b > \sqrt{n}$, then $ab > \sqrt{n}\sqrt{n} = n$ which is a contradiction to $n = ab$. Consequently, $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$, so n has a positive divisor not exceeding $\sqrt{n}$. This factor is either prime, or if it is composite itself, we may use the fundamental theorem of arithmetic to find a smaller prime factor. □

Theorem 4.19 (Infinitude of primes)**.** There are infinitely many primes.

Proof. Let us assume by contradiction that there are only finitely many primes, $p_1, p_2, \ldots, p_n$. Let

$$Q = p_1 \cdot p_2 \cdots p_n + 1$$

By the fundamental theorem of arithmetic, Q is prime or else it may be written as the product of two or more primes. However, none of the primes p_i divides Q, for if $p_i \mid Q$, then p_i divides $Q - p_1 p_2 \cdots p_n = 1$. Hence there is a prime not in the list $p_1, p_2, \ldots, p_n$, a contradiction. Consequently, there are infinitely many primes. □

Definition 4.20 (Greatest common divisor)**.** Let $a, b \in \mathbb{Z}$, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the **greatest common divisor** of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

Example 4.21. Find $\gcd(16, 40)$.

$$16 = 8 \cdot 2 \qquad 40 = 8 \cdot 5$$

so $\gcd(16, 40) = 8$.

Find $\gcd(17, 19)$. Since 17 and 19 are prime, they share no common factors other than 1, so $\gcd(17, 19) = 1$.

Definition 4.22 (Relatively prime)**.** The integers a and b are **relatively prime** if $\gcd(a, b) = 1$.

The integers $a_1, a_2, \ldots, a_n$ are **pairwise relatively prime** if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

Example 4.23 (Using prime factorization to find gcd)**.** Find $\gcd(160, 500)$.

The prime factorizations of 160 and 500 are

$$160 = 2^5 \cdot 5, \qquad 500 = 2^2 \cdot 5^3$$

then their gcd must be

$$\gcd(160, 500) = 2^{\min(5,2)} \cdot 5^{\min(1,3)} = 2^2 \cdot 5^1 = 20$$

Definition 4.24 (Least common multiple)**.** The **least common multiple** of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by $\operatorname{lcm}(a, b)$.

Example 4.25 (Using prime factorization to find lcm)**.** Find $\operatorname{lcm}(160, 500)$.

Again, since

$$160 = 2^5 \cdot 5, \qquad 500 = 2^2 \cdot 5^3$$

we see that the lcm is given by

$$\operatorname{lcm}(160, 500) = 2^{\max(5,2)} \cdot 5^{\max(1,3)} = 2^5 \cdot 5^3 = 4000$$

Remark 4.26 (General formula for gcd and lcm)**.** In general, if

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n} \qquad \text{and} \qquad b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$$

where p_i are prime numbers and $a_i, b_i \in \mathbb{N}$ for $i = 1, 2, \ldots, n$, then

$$\begin{aligned} \gcd(a, b) &= p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)} \\ \operatorname{lcm}(a, b) &= p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)} \end{aligned}$$

Theorem 4.27. Let a, b be positive integers, then

$$ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$$

END OF DAY 14

4.3 The Euclidean Algorithm

Lemma 4.28. Let $a = bq + r$, where $a, b, q, r \in \mathbb{Z}$. Then $\gcd(a, b) = \gcd(b, r)$.

Proof. If we can show that the common divisors of a and b are the same as b and r, we will have shown that $\gcd(a, b) = \gcd(b, r)$, since both pairs must have the same greatest common denominator.

Suppose that d divides both a and b. Then it follows from theorem 4.4 that d also divides $a - bq = r$. Thus a common divisor of a and b must also be a common divisor of b and r.

On the other hand suppose that d divides both b and r. Then, again by theorem 4.4, we see that d also divides $bq + r = a$. Hence, any common divisor of b and r is also a common divisor of a and b.

Consequently, $\gcd(a, b) = \gcd(b, r)$. □

Remark 4.29 (Euclidean algorithm pseudocode)**.** Suppose that a, b are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$. When we successively apply the division algorithm, starting by dividing $a = r_0$ with $b = r_1$, we have

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 && (0 \leq r_2 < r_1) \\ r_1 &= r_2 q_2 + r_3 && (0 \leq r_3 < r_2) \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n && (0 \leq r_n < r_{n-1}) \\ r_{n-1} &= r_n q_n + 0 \end{aligned}$$

Eventually, the above process will terminate with a remainder term of 0 in this sequence of successive divisions, because the sequence of remainders $a = r_0 > r_1 > r_2 > \cdots \geq 0$ cannot contain more than a term (since the must at least shrink by 1 each time). Futhermore, it follows from lemma 4.28 that

$$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$$

Hence, $\gcd(a, b)$ is the last nonzero remainder in the sequence of divisions.

Here is pseudocode for the above process, called the **Euclidean algorithm**:

```
x := a
y := b
while y != 0:
    r := x mod y
    x := y
    y := r
return x
```

Example 4.30 (Using the Euclidean algorithm)**.** Find $\gcd(414, 662)$.

Solution: Using the Euclidean algorithm, we have

$$\begin{aligned} 662 &= 414 \cdot 1 + 248 \\ 414 &= 248 \cdot 1 + 166 \\ 248 &= 166 \cdot 1 + 82 \\ 166 &= 82 \cdot 2 + \boxed{2} \\ 82 &= 2 \cdot 41 + 0 \end{aligned}$$

Hence, $\gcd(414, 662) = 2$ because 2 is the last nonzero remainder.

5 Functions

Definition 5.1 (Functions)**.** Let A, B be nonempty sets. A **function** f form A to B is an assignment of exactly one element of B to each element of A. We write $f(a) = b$ is b is the unique element of B assigned by f to the element $a \in A$. We denote the function f from A to B by $f : A \to B$.

Definition 5.2 (Domain, codomain, image, preimage)**.** If $f : A \to B$, we say that A is the **domain** and B is the **codomain** of f.

The **range**, or **image**, of f is the set of all images of elements of A. We denote the image of f by

$$f(A) = \{y \in B : \exists\, x \in A \text{ with } f(x) = y\}$$

We may also define the image of a subset of the domain, $C \subseteq A$ under f, which we similarly denote by

$$f(C) = \{y \in B : \exists\, x \in C \text{ with } f(x) = y\}$$

Last, we define the **preimage** of a subset of the codomain, $D \subseteq B$ under f as the set of elements in the domain which are mapped to D via f. We denote this set by

$$f^{-1}(D) = \{x \in A : f(x) \in D\}$$

Example 5.3 (Discrete function)**.** Let $A = \{1, 2, 3\}$ and $B = \{a, b, c, d, e\}$ and define $f : A \to B$ via the following correspondence:

$$\begin{aligned} 1 &\longrightarrow c \\ 2 &\longrightarrow e \\ 3 &\longrightarrow c \end{aligned}$$

Then we have

- A is the domain and B is the codomain.
- $f(A) = \{c, e\}$
- $f(\{1, 3\}) = \{c\}$
- $f^{-1}(B) = A$
- $f^{-1}(\{c\}) = \{1, 3\}$
- $f^{-1}(\{a, b, e\}) = \{2\}$
- $f^{-1}(\{a, b, d\}) = \varnothing$

END OF DAY 15

Example 5.4 (Continuous function)**.** Consider $f : \mathbb{R} \to \mathbb{R}$ defined by

$$f(x) = x^2$$

Then we have

- $\mathbb{R}$ is both the domain and codomain
- $f(\mathbb{R}) = [0, \infty)$ since $f(x) = x^2$ is always nonnegative
- $f(\{-2, 2\}) = \{4\}$ since $f(-2) = (-2)^2 = 4$ and $f(2) = 2^2 = 4$.
- $f([0, 5)) = [0, 25)$.
- $f^{-1}(\{3\}) = \{-\sqrt{3}, \sqrt{3}\}$
- $f^{-1}((0, 16)) = (-4, 4)$
- $f^{-1}(\{-4\}) = \varnothing$ since there does not exist $x \in \mathbb{R}$ such that $f(x) = x^2 = -4$.

Note in the last point above, if we chose $f : \mathbb{C} \to \mathbb{R}$, then $f^{-1}(\{-4\}) = \{2i\}$ since $f(2i) = (2i)^2 = 4i^2 = -4$.

Remark 5.5 (Careful considerations)**.** Be careful to note that functions must be defined with their domain and codomain already stated and known. This is counterintuitive to questions seen in previous courses (calculus, precalculus, algebra, etc) which would ask you to find a function's domain.

Technically, the functions we tried to find the domain of were considered **partial functions** and we were being asked to find their **natural domain**. In application, most "functions" you may deal with will be some kind of partial function.

Remark 5.6 (Codomain considerations)**.** If $f : A \to B$ is a function, then we must have that $f(A) \subseteq B$. It would not make sense otherwise.

Thus, there is some need to know how f behaves on A in order to state what B is. In general, you may state the codomain to be as large of a set as you'd like. For example if your function outputs numbers, then you can just have your codomain be $\mathbb{C}$ all the time to be safe, although some may find this not very descriptive. Another not very descriptive way of defining your functions is to always write

$$f : A \to f(A)$$

which is certainly correct, but again, not very helpful.

Definition 5.7 (Injective)**.** Let $f : A \to B$. Then the function f is said to be **one-to-one** or **injective** if $f(a) = f(b)$ implies that $a = b$ for all $a, b \in A$.

Example 5.8 (Injective example)**.** Consider $f : \{a, b, c, d\} \to \{1, 2, 3, 4, 5\}$ with $f(a) = 2$, $f(b) = 1$, $f(c) = 5$, and $f(d) = 3$. Since no two elements of $\{a, b, c, d\}$ are mapped to the same element by f, then we have that f is injective.

Example 5.9 (Not injective example)**.** Consider $f : \{a, b, c, d\} \to \{1, 2, 3, 4, 5\}$ with $f(a) = 2$, $f(b) = 1$, $f(c) = 5$, and $f(d) = 2$. Since $f(a) = f(d) = 2$, but $a \neq d$ then we say that f is not injective.

Definition 5.10 (Surjective)**.** A function $f : A \to B$ is called **onto** or **surjective** if for every element $b \in B$, there is an element $a \in A$ with $f(a) = b$.

Example 5.11 (Surjective example)**.** Consider $f : \{1, 2, 3, 4\} \to \{a, b, c, d\}$ with $f(1) = d$, $f(2) = b$, $f(3) = c$, $f(4) = a$. Then since a, b, c, d are all attained by f, we have that f is surjective.

Example 5.12 (Not surjective example)**.** Consider $f : \{1, 2, 3, 4\} \to \{a, b, c, d\}$ with $f(1) = d$, $f(2) = b$, $f(3) = a$, $f(4) = a$. Then since c is not attained by f, we have that f is not surjective.

Example 5.13 (Injective, surjective dependent on choice of domain, codomain)**.** Let $f : \mathbb{R} \to \mathbb{R}$ be defined by x^2. Then since our codomain is defined as $\mathbb{R}$, we know that $-1 \in \mathbb{R}$, but there does not exist any $x \in \mathbb{R}$ such that

$$f(x) = x^2 = -1$$

so as defined, f is not surjective. Next, since $f(-2) = f(2)$, we know that f is not injective.

If we define $f : [0, \infty) \to \mathbb{R}$ by $f(x) = x^2$, then we still have that f is not surjective, but we may now prove that f is injective.

Proof. Let $x, y \in [0, \infty)$ and suppose that $f(x) = f(y)$. Then by definition,

$$x^2 = y^2$$

If one of x or y is zero, then we must have that $x = y = 0$. Otherwise, if x and y are both not zero, then

$$x^2 = y^2 \iff x^2 - y^2 = 0 \iff (x + y)(x - y) = 0$$

If $x + y = 0$, then $x = -y$ which contradicts that $x, y > 0$, so we must have $x - y = 0$ or $x = y$. Thus, f is injective. □

If we now define $f : [0, \infty) \to [0, \infty)$ by $f(x) = x^2$, then injectivity holds from the previous example, and we can now prove that f is surjective.

Proof. Let $y \in [0, \infty)$ (codomain). Then since $y \geq 0$, we know that $\sqrt{y}$ is defined and nonnegative. Thus, $\sqrt{y} \in [0, \infty)$ (domain), and we see that

$$f(\sqrt{y}) = (\sqrt{y})^2 = y$$

which proves that f is surjective. □

To summarize

1. $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = x^2$ is $\begin{cases} \text{Not injective} \\ \text{Not surjective} \end{cases}$

2. $f : [0, \infty) \to \mathbb{R}$ with $f(x) = x^2$ is $\begin{cases} \text{Injective} \\ \text{Not surjective} \end{cases}$

3. $f : [0, \infty) \to [0, \infty)$ with $f(x) = x^2$ is $\begin{cases} \text{Injective} \\ \text{Surjective} \end{cases}$

Remark 5.14 (Proof technique for injectivity and surjectivity)**.** Suppose that $f : A \to B$.

1. To show that f is injective: Show that if $f(x) = f(y)$ for arbitrary $x, y \in A$, then $x = y$.

2. To show that f is not injective: Find particular elements $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$.

3. To show that f is surjective: Consider an arbitrary element $y \in B$ and prove there exists an element $x \in A$ such that $f(x) = y$.

4. To show that f is not surjective: Find a particular $y \in B$ such that $f(x) \neq y$ for all $x \in A$.

Definition 5.15 (Bijection)**.** A function $f : A \to B$ is called a **bijection** if it is both injective and surjective. We also say that the function f is **bijective**.

Remark 5.16 (Bijections lead to inverses)**.** Consider a bijection $f : A \to B$. Then since f is surjective, every element $y \in B$ is mapped to by some element in $x \in A$. Furthermore, because f is injective, every element $y \in B$ is mapped to by a unique element $x \in A$. Thus, we can define a new function from B to A which reverses the mapping done by f.

END OF DAY 16

Definition 5.17. Let $f : A \to B$ be a bijection. The **inverse function** of f is the function which assigns to an element $b \in B$, the unique element $a \in A$ such that $f(a) = b$. The inverse function of f is denoted f^{-1}. Hence $f^{-1}(b) = a$ when $f(a) = b$.

Example 5.18 (Discrete bijection and inverse)**.** Let f be the function from $\{a, b, c\}$ to $\{1, 2, 3\}$ such that

$$f(a) = 2, \quad f(b) = 3, \quad f(c) = 1$$

Then f is surjective since 1,2,3 are all attained and f is injective since no two elements of a, b, c are mapped to the same element. Furthermore, we see that all elements in $\{1, 2, 3\}$ are attained from $\{a, b, c\}$ via f. Thus, f is a surjection. Hence f is a bijection, so f^{-1} exists.

The inverse of f is then given by $f^{-1} : B \to A$ such that

$$f^{-1}(1) = c, \quad f^{-1}(2) = a, \quad f^{-1}(3) = b$$

Example 5.19 (Continuous bijection and inverse)**.** Let $f : [0, \infty) \to [0, \infty)$. In example 5.13, we have shown that f is injective and surjective, hence a bijection. Thus, f has an inverse given by

$$f^{-1}(y) = \sqrt{y}$$

Definition 5.20 (Composition)**.** Let g be a function from sets $A \to B$ and let f be a function from sets $B \to C$. The **composition** of the functions f and g, denoted for all $a \in A$, by $f \circ g$, is the function from $A \to C$ defined by

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

Example 5.21 (Discrete composition)**.** Let $g : \{+, \times, \%\} \to \{1, 2, 3\}$ given by

$$\begin{aligned} + &\longrightarrow 3 \\ \times &\longrightarrow 1 \\ \% &\longrightarrow 1 \end{aligned}$$

and $f : \{1, 2, 3\} \to \{a, b, c\}$ given by

$$\begin{aligned} 1 &\longrightarrow b \\ 2 &\longrightarrow a \\ 3 &\longrightarrow c \end{aligned}$$

then $(f \circ g) : \{+, \times, \%\} \to \{a, b, c\}$ is given by

$$\begin{aligned} (f \circ g)(+) &= f(g(+)) = f(3) = c \\ (f \circ g)(\times) &= f(g(\times)) = f(1) = b \\ (f \circ g)(\%) &= f(g(\%)) = f(1) = b \end{aligned}$$

Remark 5.22 (More on this chapter)**.** There's much more that can be said about properties of compositions and functions in general, but we are unfortunately out of time for this section.

6 Cardinality

Definition 6.1 (Equal cardinality)**.** Two sets, A, B have the same cardinality if there exists a bijection $f : A \to B$. When A and B have the same cardinality, we write $|A| = |B|$.

Remark 6.2. Note that it is clear when two finite sets have the same cardinality because we can just count the number of elements in each. Definition 6.1 allows us to now compare the sizes of sets with infinite cardinality. This hints that there are infinite sets that don't have the same cardinality, i.e., one infinity being "bigger" than another infinity.

Definition 6.3 (Smaller cardinality)**.** Let A, B be sets. If there is an injection $f : A \to B$, then the cardinality of A is less than or the same as the cardinality of B and we write $|A| \leq |B|$. Moreover, if $|A| \leq |B|$ and A and B have different cardinality, then we say the cardinality of A is less than the cardinality of B and we write $|A| < |B|$.

6.1 Countable sets

Definition 6.4 (Countable and uncountable)**.** A set that is either finite or has the same cardinality as the set of positive integers, $\mathbb{Z}^+$, is called **countable**. A set that is not countable is called **uncountable**. When an infinite set S is countable, we denote the cardinality of S by $\aleph_0$ (where $\aleph$ is "aleph", the first letter of the Hebrew alphabet). We write $|S| = \aleph_0$ and say that S has cardinality "aleph null".

Remark 6.5 (Georg Cantor)**.** The reason we use a Jewish letter to denote higher cardinality is due to the founder of set theory, Georg Cantor (1845-1918). He made the discovery that there were different types of infinite sets.

Theorem 6.6. If $A \subseteq B$, then $|A| \leq |B|$.

Example 6.7 (Odds are countable)**.** Show that the set of odd positive numbers is a countable set.

To show that the set of odd positive numbers is countable, we will construct a bijection between this set and the positive integers, $\mathbb{Z}^+$. Consider the function

$$f(n) = 2n - 1$$

from $\mathbb{Z}^+$ to the odd positive numbers. To see that f is injective, suppose that $f(n) = f(m)$ for $n, m \in \mathbb{Z}^+$. Then

$$2n - 1 = 2m - 1 \iff n = m$$

To see that f is surjective, let t be an odd positive number, then t is one less than an even number $2k$ where $k \in \mathbb{Z}^+$. Thus, $t = 2k - 1 = f(k)$. Hence, f is a bijection.

From this example, we see that the set of positive odd integers is the same "size" as the the set of all positive integers.

Remark 6.8 (Countability)**.** An infinite set S is countable if and only if it is possible to list the elements of S in a sequence (indexed by the positive integers), i.e., it is possible to write

$$S = \{a_1, a_2, a_3, \dots\}$$

since we can define a bijection $f : \mathbb{Z}^+ \to S$ by $f(i) = a_i$ for $i \in \mathbb{Z}^+$.

This is where the term "countable" comes from since there is a possibility, that given infinite time, one could count all the elements in a countable set. Whereas for an uncountable set, there is no such possibility, i.e., it is impossible to come up with a method of counting its elements.

Example 6.9 (Hibert's hotel)**.** The Mathematician David Hilbert (1862-1943) invented the thought experiment known as the **Grand Hotel**, which has a countably infinite number of rooms (labeled room 1, room 2, etc), each currently occupied by a guest. Now say that a new guest arrives and is asking for a room. In order to accomodate them without evicting any current guest and without requiring anyone move more than once nor move an infinite distance, Hilbert came up with the following solution:

Have each current guest shift over by 1 room. That is, the guest in room 1 moves to room 2, the guest in room 2 moves to room 3, and so on. This frees up room 1 for the new guest to move in and no one is left without a room.

The above notion is analagous to saying that

$$|\underbrace{\{1,2,3,\dots\}}_{\mathbb{Z}^+}| = |\{2,3,4,\dots\}|$$

END OF DAY 17

Let us now consider the following scenarios

1. Suppose now instead of 1 new guest, a bus containing $n \in \mathbb{Z}^+$ new guests arrive. How can the Grand Hotel accomodate them without evicting any current guest?

   Solution: Instead of shifting all the guests by one room, shift them by n rooms. That is the guest in room 1 moves to room $n+1$, the guest in room 2 moves to room $n+2$, and so on. This frees up rooms 1 to n for the new guests to move in.

2. Suppose that a bus containing a countably infinite number of new guests arrives at the Grand Hotel. How can all of these guests be accomodated without evicting any current guest?

   Solution: We can exploit the even and odd numbers to accomodate everyone. Have the current guests move in the following way:

$$\begin{gathered} 1 \longrightarrow 2 \\ 2 \longrightarrow 4 \\ 3 \longrightarrow 6 \\ \vdots \end{gathered}$$

   This moves all the current guests into even numbered rooms which frees up the odd numbered rooms for the countably infinite number of new guests

3. Suppose a countably infinite number of buses arrive, where each bus contains a countably infinite number of new guests. How can we accomodate everyone in each bus all at once without evicting any current guest?

   Solution: We can exploit prime numbers to accomodate everyone. Let us denote the infinite number of buses by bus 1, bus 2, and so on. Next, for the current guests, have the guest in room i move to room 2^i. That is

$$\begin{aligned} 1 &\longrightarrow 2 \\ 2 &\longrightarrow 2^2 \\ 3 &\longrightarrow 2^3 \\ &\vdots \end{aligned}$$

   then have guest i in bus 1 move to room 3^i, guest i in bus 2 move to room 5^i, and so on. Note that this solution leaves a countably infinite number of rooms vacant, i.e., any room that's not a power of a prime number (like 6,10, 12, etc).

   Hence, somehow, an infinite number of infinitely full buses can fit into the fully occupied Grand Hotel, which is just the size of one of those buses, and there will be an infinite number of vacancies after everyone has settled into their room.

Example 6.10 (Programs in a language)**.** The set of all possible programs that may be written in any programming language is countable.

Example 6.11 (Rationals are countable)**.** $\mathbb{Q}$ is countable.

Idea: We can enumerate the positive rationals by placing them into a matrix type of structure. The trick is to let each diagonal represent all rationals whose numerator and denominator sum up to n for $n > 1$. By this I mean the following:

A rational number takes the form $\frac{p}{q}$ where $p, q \in \mathbb{Z}$. Let S_n for $n > 1$ be the set

$$S_n = \left\{ \frac{p}{q} \in \mathbb{Q} : p + q = n,\ p/q \text{ is not reduced} \right\}$$

Some examples:

$$\begin{aligned} S_2 &= \left\{ \frac{1}{1} \right\} \\ S_3 &= \left\{ \frac{1}{2}, \frac{2}{1} \right\} \\ S_4 &= \left\{ \frac{1}{3}, \frac{2}{2}, \frac{3}{1} \right\} \\ S_5 &= \left\{ \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1} \right\} \end{aligned}$$

Thus, we have that we can display all the rational by

$$\begin{array}{cccccc}
\frac{1}{1} & \frac{2}{1} & \frac{3}{1} & \frac{4}{1} & \frac{5}{1} & \cdots \\
\frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \frac{4}{2} & \frac{5}{2} & \cdots \\
\frac{1}{3} & \frac{2}{3} & \frac{3}{3} & \frac{4}{3} & \frac{5}{3} & \cdots \\
\frac{1}{4} & \frac{2}{4} & \frac{3}{4} & \frac{4}{4} & \frac{5}{4} & \cdots \\
\frac{1}{5} & \frac{2}{5} & \frac{3}{5} & \frac{4}{5} & \frac{5}{5} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

and we can count by snaking along each diagonal.

6.2 Uncountable sets

Example 6.12 ($\mathbb{R}$ is uncountable)**.** Show that the set of real numbers is uncountable.

We will proceed by a famous proof technique known as the **Cantor diagonalization argument**.

Proof. To show that $\mathbb{R}$ is uncountable, we proceed by contradiction. Indeed, suppose that $\mathbb{R}$ is countable. Then since $(0,1) \subset \mathbb{R}$ and $(0,1)$ is infinite, then $(0,1)$ must also be countable.

Thus, we can list the elements in $(0,1)$ by $r_1, r_2, \dots$ and we also note that each $r_i \in (0,1)$, being a positive number less than 1, has a decimal expansion. Thus, we have

$$\begin{aligned}
r_1 &= 0.d_{11}d_{12}d_{13}\dots \\
r_2 &= 0.d_{21}d_{22}d_{23}\dots \\
r_3 &= 0.d_{31}d_{32}d_{33}\dots \\
r_4 &= 0.d_{41}d_{42}d_{43}\dots \\
&\vdots
\end{aligned}$$

where d_{ij} is a digit in the set $\{0,1,2,3,4,5,6,7,8,9\}$. Next, we will define a new number r, by

$$r = 0.(d_{11} +_{10} 1)(d_{22} +_{10} 1)(d_{33} +_{10} 1)\dots$$

Since $(0,1)$ is a set, then each r_i has a unique decimal expansion. Since the ith digit in r is given by $d_{ii} +_{10} 1$, we know that $r \neq r_i$ for all $i \in \mathbb{Z}^+$. Thus, r is a real number strictly between 0 and 1 that is not contained in (0,1), a contradiction. Thus, $\mathbb{R}$ is not countable, hence uncountable. □

Theorem 6.13 (Cantor-Schröder-Bernstein Theorem)**.** Let A, B be sets. If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

In other words, instead of constructing a bijection between A and B, we can instead just construct injections in both directions.

Theorem 6.14 (Cantor's Theorem)**.** If A is any set, then $|A| < |\mathscr{P}(A)|$.

Remark 6.15 (Continuum Hypothesis)**.** We conclude the course with a brief discussion about a famous open problem about cardinality.

From Cantor's theorem, we see that we can build an infinite sequence of higher and higher cardinalities beyond $\aleph_0$ by

$$\aleph_0 = |\mathbb{Z}^+| < |\mathscr{P}(\mathbb{Z}^+)| < |\mathscr{P}(\mathscr{P}(\mathbb{Z}^+))| < |\mathscr{P}(\mathscr{P}(\mathscr{P}(\mathbb{Z}^+)))| < \cdots$$

For each of these, we assign the following symbol to each

$$\begin{aligned} |\mathbb{Z}^+| &= \aleph_0 \\ |\mathscr{P}(\mathbb{Z}^+)| &= \aleph_1 \\ |\mathscr{P}(\mathscr{P}(\mathbb{Z}^+))| &= \aleph_2 \\ |\mathscr{P}(\mathscr{P}(\mathscr{P}(\mathbb{Z}^+)))| &= \aleph_3 \\ &\vdots \end{aligned}$$

The following two properties can be proved:

1. $\aleph_0$ is the smallest an infinite set can be.
2. $|\mathbb{R}| = \aleph_1$, so uncountably infinite sets are only tier-2 among the countable hierarchy of infinities.

Now, in mathematics, there is a trend of discrete type objects eventually expanding into continuous type objects.

- In number theory, it was originally thought that there were no numbers beyond $\mathbb{Q}$ until Pythagoras (and many others) discovered the existance of irrationals (like $\sqrt{2}$).
- In geometry, it was originally thought that dimensions were restricted to $\mathbb{N}$ (i.e., dimension 0,1,2,3,4,etc.), but it was eventually discovered that certain objects exist in dimensions that are strictly between the usual physical dimensions (like dimension $1 < \log_2(3) < 2$)

It is possible that this same trend applies to higher cardinalities; that there could be infinite sets whose cardinality was strictly between $\aleph_0$ and $\aleph_1$, i.e. something strictly between countable and uncountable. Cantor's hypothesis, the **Continuum Hypothesis** is actually the statement that no such set exists. Cantor spent most of his life researching this problem, discovering many groundbreaking results in set theory, but eventually went clinically insane. He died in 1918 without resolving the problem.