مدرسہ ریاضیات

Habib Math Club

Logic and Proofs

Summer 2024

In this chapter, we go over some prerequisite knowledge that will be required in later sessions. For further reading related to this session refer to chapter 1 and chapter 5 of the book Discrete Mathematics and Its Applications by Kenneth H. Rosen [?]. For the following sessions, we will follow the schedule given in the table below. First, we will introduce classical propositional and predicate logic, then we look at the notion of mathematical proofs. What is a mathematical proof? What makes a proof valid? With these we will look at some proof techniques.
The references section gives us the textbooks recommended for this course.

Logic

Logic is used to build symbolic models of our world. We build models so we can formally describe and reason about this universe. In itself logic lies outside reality, we build the rules and principles of logic around our intuitive understanding of reality, but the logic itself lies outside it. Classical logic was created to give precise meaning to mathematical statements and give reasoning principles for mathematics. We build our system of logic based on natural language, the sentences we use to reason, such as “I had two air fryers, and I bought three more air fryers therefore now I have five air fryers”.
In mathematics we want a statement to be either true or false. The logic that builds on this is called two-valued logic. As we move along this chapter we look into some more principles of classical two-values logic.

Proposition

Propositions are declarative statements, they are sentences with a certain truth value, and they are either true or false. Some examples of propositions can be: $P_1 : 1 + 2 = 3$, P_2 : *Everyone loves Speedwagon.*, P_3 : *I am duck.*. A non-example of propositions is a sentence like, *Am I a duck?*. Propositional logic is also known as Zeroth order logic.

Problems

1. 1

Which of the following are propositions?

(a) $2 \times 5 = 10$

(b) $52 + 48 = 100$

(c) $2 - 3 = 1$

(d) What's my purpose?

(e) 0.420420420420 is a real number.

(f) $\textsf{\textbf{P}} = \textsf{\textbf{NP}}$

(g) Wubba lubba dub dub

(h) There are no odd perfect numbers.

(i) Answer to the Ultimate Question of Life, the Universe, and Everything is 42.

(j) Danger is my middle name.

(k) Come here wabbit.

(l) 14 is a prime number.

(m) What is the answer to the Ultimate Question of Life, the Universe, and Everything?

(n) KHAAAAAAAAAAN!!!

(o) He tasks me. He tasks me and I shall have him! I'll chase him around the moons of Nibia and round the Antares Maelstrom and round Perdition's flames before I give him up!

(p) This statement is false.

(q) Kermit is in gamer rage.

(r) Shrek is adorable.

Connectives

Now with just propositions we can do much, we need connectives to meaningfully reason about these propositions. We also use them to create new propositions from old ones. These connectives are attributed to George Boole, as they were discussed in his 1854 book, The Laws of Thought. The area of logic that deals with propositions is called propositional calculus.

Negation

In everyday language we are often interested in the negation of things, we say X is true while Y is not true. So if I say Y is not true then *not* Y must be true. So logical negation is defined as follows.

Definition 1. *Let p be a proposition. The negation of p, denoted by $\neg p$, and read as "not p", is the statement "p is false". The truth value of $\neg p$ is the opposite of the truth value of p.*

Table of negation	
p	$\neg p$
T	**F**
F	**T**

Conjunction

In everyday language, we are often interested in statements involving two propositions such as we want to declare that both these propositions are true. For this we often use the word "and", we say X and Y are true. So logical conjunction also known as "and" is defined as follows.

Definition 2. *Let p and q be propositions. The conjunction of p and q, denoted by $p \wedge q$, read as "p and q", is true when both p and q are true and is false otherwise.*

Table of conjunction		
p	q	$p \wedge q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**F**
F	**F**	**F**

Disjunction

In everyday language, we are often interested in statements involving two propositions such as when we want to declare that either of these propositions is true. For this we often use the word "or", we say X or Y is true. So logical disjunction also known as "or" is defined as follows. (It is to note that logical "or" is different from the English word "or")

Definition 3. *Let p and q be propositions. The disjunction of p and q, denoted by $p \vee q$, read as "p or q", is false when both p and q are false and is true otherwise.*

Table of disjunction		
p	q	$p \vee q$
T	**T**	**T**
T	**F**	**T**
F	**T**	**T**
F	**F**	**F**

Implication

In order to meaningfully reason about statements we like to use conditional statements. We like to say things like "If X is true then Y will be true", so with this, we can reason and say "If X is true then Y will be true, so as X is true therefore Y is true". For this we use implications, logical implication is defined as follows.

Definition 4. *Let p and q be propositions. The implication p implies q, denoted by $p \implies q$, read as "p implies q", says if p is true then q must be true.*

Table of implication		
p	q	$p \implies q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**T**
F	**F**	**T**

$p \implies q$ is logically equivalent to $\neg p \vee q$. For an implication $p \implies q$, $\neg q \implies \neg p$ is known as the contrapositive if $p \implies q$ is true then so is $\neg q \implies \neg p$. $q \implies p$ is called the converse of $p \implies q$ and $\neg p \implies \neg q$ is called the inverse. The converse and inverse are not necessarily true if the implication is true.
When expressing implication in natural language, we like to use words such as "necessary" and "sufficient". For implications $p \implies q$, we say p is sufficient for q and q is necessary for p.

Biconditional

Often times we are interested if two statements are logically equivalent. This is also known as biconditional. We say "X is equivalent to Y" that is "If X is true then Y is true and if Y is true then X is true". This is also often called if and only if statement (often if and only if is shortened as "iff"). We say "X is true if and only if Y is true". Biconditional is formally defined as:

Definition 5. *Let p and q be propositions. The biconditional p iff q, denoted by $p \iff q$, read as "p if and only if q", says if p is true then q must be true and if q is true then p must be true. In other words, $p \iff q$ is true if p and q have the same truth value.*

Table of biconditional		
p	q	$p \iff q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**F**
F	**F**	**T**

For the statement $p \iff q$ we say p is necessary and sufficient for q and q is necessary and sufficient for p.

Problems

1. 1

Construct the truth table of $(p \implies q) \wedge (\neg p \implies q)$.

2. 2

The logical connective xor $\oplus$ (read as exclusive or) is defined as, for propositions p and q, $p \oplus q$ is true if exactly one of p or q is true and is false otherwise. express $\oplus$ in terms of negation, conjunction and disjunction.

Predicates

We can see that just propositional logic is not sufficient to express all mathematical statements meaningfully. Let's take statements such as "For all integers x greater than 1, $x + 1$ is a positive integer", we can't evaluate this statement's truth value using propositional logic. For this we use predicates. Predicate logic is also known as first-order logic.

While propositional logic deals with simple declarative propositions, In predicate logic, we have two additional elements called predicates and qualifiers. Predicates are statements that contain a variable. For example let $P(x)$ be a predicate, let $P(x)$: *x+3 = 5.* Unlike propositions, a predicate evaluates to true or false for an entity or entities in the domain of discourse. Once a value has been assigned to the variable x, the statement $P(x)$ becomes a proposition and has a truth value. For example $P(2)$: *2+3 = 5* is true, while $P(3)$: *3+3 = 5* is false. Here P is also called the propositional function. It is to be noted that predicate logic is a superset of propositional logic, so every proposition is also a predicate.

Quantifiers

Certain times we like to make statements such as "for all x, $P(x)$ is true", or "there is a x, such that $P(x)$ is true", we like to quantify the variable of our propositional function. We have two fundamental quantifiers, the universal quantifier and the existential quantifier. We define them as follows.

Definition 6. *The universal quantification of $P(x)$ is the statement "for all values of x in the domain $P(x)$ is true". We denote this as $\forall x P(x)$. $\forall$ symbol is called the universal quantifier. An element for which $P(x)$ is false is called a counterexample to $\forall x P(x)$.*

Definition 7. *The existential quantification of $P(x)$ is the statement "there is a value of x in the domain such that $P(x)$ is true". We denote this as $\exists x P(x)$. $\exists$ symbol is called the existential quantifier.*

Let's say I want to say that if we sum any two real numbers the number we obtained is also a real number. We can formally express this statement in predicate logic as; let $P(x, y)$: $x + y \in \mathbb{R}$, where $\mathbb{R}$ is the symbol for the set of real numbers, then we can say that $\forall x, y \in \mathbb{R}, P(x, y)$. Similarly, if I want to say that there is a real number such as it summed with 1 equals two we can express it in predicate logic as; let $Q(x)$: $x + 1 = 2$, then we can say that $\exists x \in \mathbb{R}, Q(x)$.

Problems

1. 1

Express the following statements in predicate logic:

(a) "Everyone thinks Shrek is adorable."

(b) "Someone saw Kermit in gamer rage."

(c) "There are real number a, b, c such that $a^2 + b^2 = c^2$."

(d) "For any natural number there exists another natural number such that their sum is equal to 0."

(e) "All horses are the same colored but there is a donkey that is brown."

2. 2

Negate the following statements in predicate logic:

(a) $\forall x P(x)$.

(b) $\exists x P(x)$.

(c) $\forall x \exists y P(x, y)$.

(d) $\exists x \forall x P(x, y)$.

3. 3

The uniqueness quantifier $\exists!$ is defined as, let $P(x)$ be a predicate then $\exists! x P(x)$ says that, there exists a unique x in the domain such that $P(x)$ is true. In other words $P(x)$ is true for exactly one x in the domain. Express $\exists! x P(x)$ in terms of universal and existential quantifiers. (Use logical connectives)

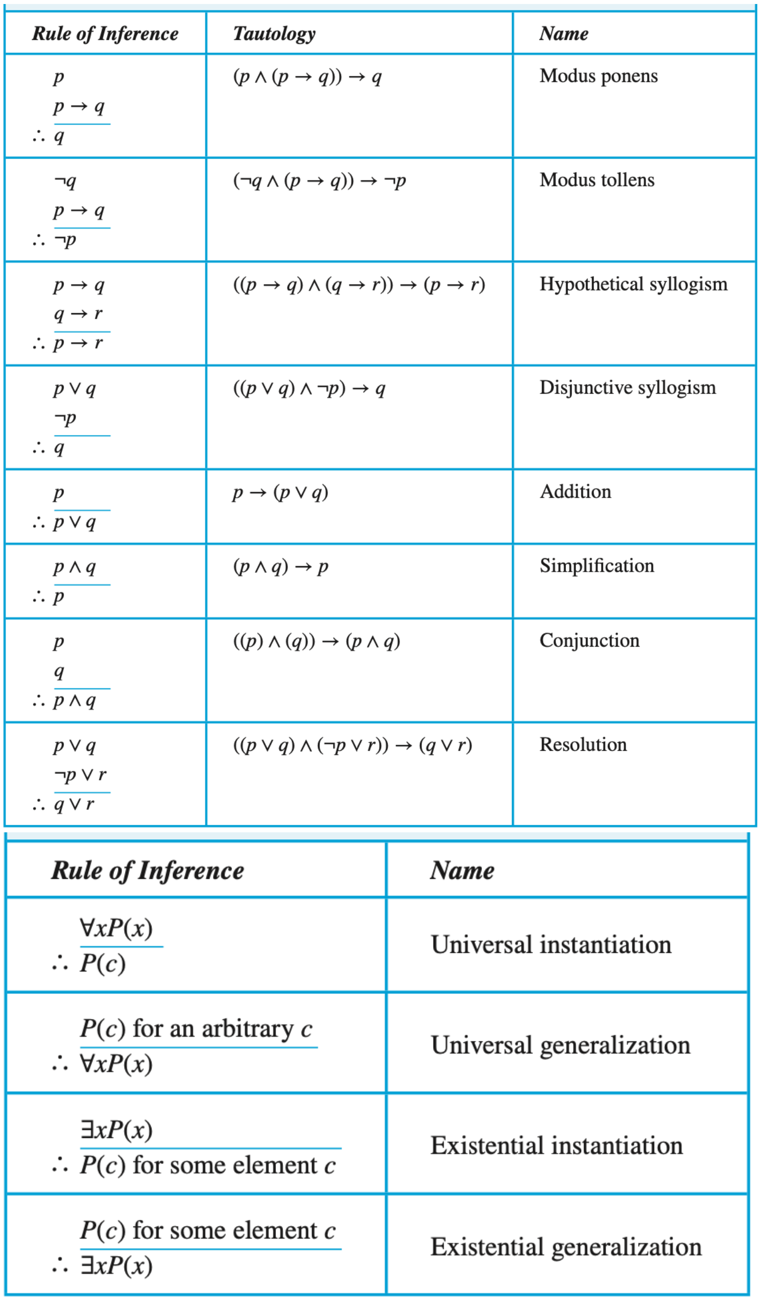
Laws of logic

There are some laws of logic that we must keep in mind. The two most fundamental laws are known as non-contradiction and excluded middle. A compound proposition that is always true, no matter what the truth values of the propositional variables that occur in it, is called a tautology. A compound proposition that is always false is called a contradiction. A compound proposition that is neither a tautology nor a contradiction is called a contingency. The compound propositions p and q are called logically equivalent if $p \iff q$ is a tautology. The notation $p \equiv q$ denotes that p and q are logically equivalent. We like to know the logical equivalences of some statements which we call laws. The following table gives a list of these laws.

Table of logical equivalences/laws	
Equivalence	Name
$p \wedge \neg p \equiv \mathbf{F}$	Law of non-contradiction
$p \vee \neg p \equiv \mathbf{T}$	Law of excluded middle
$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	Identity laws
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws
$(p \vee q) \vee r \equiv p \vee (p \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (p \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws

Inference

With all these basic principles of first-order logic, we would like to argue about things and reach certain conclusions from a premise. For this, we need the rules of inference. These rules define how we can infer a conclusion from a premise. The following tables give us these rules of inference.



Rule of Inference	*Tautology*	*Name*
p $p \to q$ $\therefore q$	$(p \wedge (p \to q)) \to q$	Modus ponens
$\neg q$ $p \to q$ $\therefore \neg p$	$(\neg q \wedge (p \to q)) \to \neg p$	Modus tollens
$p \to q$ $q \to r$ $\therefore p \to r$	$((p \to q) \wedge (q \to r)) \to (p \to r)$	Hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore q$	$((p \vee q) \wedge \neg p) \to q$	Disjunctive syllogism
p $\therefore p \vee q$	$p \to (p \vee q)$	Addition
$p \wedge q$ $\therefore p$	$(p \wedge q) \to p$	Simplification
p q $\therefore p \wedge q$	$((p) \wedge (q)) \to (p \wedge q)$	Conjunction
$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	$((p \vee q) \wedge (\neg p \vee r)) \to (q \vee r)$	Resolution

Rule of Inference	*Name*
$\forall x P(x)$ $\therefore P(c)$	Universal instantiation
$P(c)$ for an arbitrary c $\therefore \forall x P(x)$	Universal generalization
$\exists x P(x)$ $\therefore P(c)$ for some element c	Existential instantiation
$P(c)$ for some element c $\therefore \exists x P(x)$	Existential generalization

Figure 1: Table of rules of inference. The tables are taken from Discrete Mathematics and Its Applications by Kenneth H. Rosen [?].

Problems

1. 1

You're a bizarre adventure with Johnny Joestar to stop the president of the United States. You need to find pieces of the corpse of a saint. The adventure leads you to an island inhabited by knights, who always tell the truth, and knaves, who always lie. Gyro Zeppeli tells you that a piece is in a cave. The cave is guarded by two enemy stand users A and B, who are inhabitants of the island (they are either knights or knaves). They will only let you into the cave if you can determine, if possible, what A and B are if they address you in the ways described.

(a) A says “At least one of us is a knave” and B says nothing.

Solution: If A is a knave, then they are telling the truth as there does indeed exist at least one knave. But knaves always lie, so A cannot be a knave. Then A is a knight. Knights always tell the truth, therefore, there must indeed be a knave among the two. A cannot be a knave, therefore B is a knave.

(b) A says “The two of us are both knights” and B says “A is a knave”.

Solution: If A is a knight, then A’s statement must be true. However, B’s statement contradicts A’s statement. So B cannot be a knight, and this case is false. However, if B is a knave, then B is telling a lie, which contradicts A’s statement, therefore, A’s statement cannot be true. So this case is false. If A is a knave, and B is a knave, then B is telling the truth, so this can’t be the case. Then if A is a knave, and B is a knight, there is no contradiction here, as A is telling a lie which holds as a knave must always tell lies, and B is telling the truth that A is a knave. Therefore, A is a knave and B is a knight.

(c) A says “I am a knave or B is a knight” and B says nothing.

Solution: If A is a knave, then he is telling the truth about himself, that he is a knave which implies his statement is true. But knaves always lie, so his statement should be false, therefore A cannot be a knave. Then A is a knight. Now we know that A is a knight, so A’s statement, “I am a knave” is not true, so for the statement to be true, “B is a knight” must be true.
Then it can be concluded that A is a knight, and B is a knight.

(d) Both A and B say “I am a knight”

Solution: It cannot be determined as both statements can hold in either scenario. If A is a knight, he is telling the truth so is true, but if A is not a knight, he is lying which means he is a knave, which is also true.
The same argument holds for B, therefore A and B cannot be determined.

(e) A says we “We are both knaves ” and B says nothing.

Solution: If A is a knight, then this statement is false by the rules of the knight, therefore A is not a knight. So A must be a knave. A is a knave, then A’s statement must be a lie and both cannot be knaves. Since A is a knave, then B cannot be a knave so B is a knight. A is a knave and B is a knight.

2. 2

Three Vulcans walk into the mess hall of the starship enterprise. Spock approaches them with a cake and asks "Does everyone want some cake?" The first Vulcan says "I don't know". The second Vulcan says "I don't know". Finally, the third Vulcan says "No". Spock comes back and gives slices of cake to the Vulcan who wanted cake. How did Spock figure out who wanted the cake? (The Vulcans are a humanoid species from the planet Vulcan. They are widely renowned for their strict adherence to logic and reason as well as their remarkable stoicism. Spock is also a Vulcan.)

3. 3

Professor Paradox has been taken captive by Eon. In order to save him you need to find his Chrononavigator which he hid somewhere. Lucky for you, he left clues behind to find the Chrononavigator. By using the following clues deduce where the Chrononavigator is hidden.

- If Mr.Smoothy is next to a Burger Shack, then the Chrononavigator is in the Plumber's headquarters.
- If Mr.Smoothy is not next to a Burger Shack or the Chrononavigator is buried under Baumann's Store, then the tree in the front of Billion Tower is an elm and the tree in the back of Billion Tower is not an oak.
- If the Chrononavigator is in the Argistix Security office, then the tree in the back of Billion Tower is not an oak.
- If the Chrononavigator is not buried under Baumann's Store, then the tree in front of Billion Tower is not an elm.
- The Chrononavigator is not in the Plumber's headquarters.

Using rules of inference, determine where the Chrononavigator is hidden. Clearly state what your propositions represent.

Solution:

4. 4

Show that the following are logically equivalent without using truth tables

(a) $(p \implies r) \vee (q \implies r) \equiv (p \wedge q) \implies r$

Solution: $(p \implies r) \vee (q \implies r) \equiv (p \wedge q) \implies r$

LHS:

$\neg((p \implies r) \vee \neg(q \implies r))$ $[\neg(A \vee B) \equiv \neg A \wedge \neg B]$

$(p \wedge \neg r) \wedge (q \wedge \neg r)$ $[\neg(p \implies q) \equiv p \wedge \neg q]$

$(p \wedge q) \wedge \neg r$ [Distributive Law]

$(p \wedge q) \implies r$ $[\neg(p \implies q) \equiv p \wedge \neg q]$

RHS:

$\neg((p \wedge q) \implies r)$

$(p \wedge q) \wedge \neg r$
$(p \wedge \neg r) \wedge (q \wedge \neg r)$
$\neg((p \wedge \neg r) \wedge (q \wedge \neg r))$
$\neg(p \wedge \neg r) \vee \neg(q \wedge \neg r)$
$\neg\neg(p \implies r) \vee \neg\neg(q \implies r)$
$(p \implies r) \vee (q \implies r)$

(b) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge) r$

(c) $\neg[\neg[(p \vee q) \wedge r] \vee \neg q] \equiv q \wedge r$

(d) $(p \vee q \vee r) \wedge (p \vee t \vee \neg q) \wedge (p \vee \neg t \vee r) \equiv p \vee [r \wedge (t \vee \neg q)]$

Proofs

When we talk about mathematical statements we need to "prove" their validity. If I make a mathematical assertion I need to be able to show that the assertion is indeed true. A proof is a valid argument that establishes the truth of a mathematical statement. A theorem is a statement that is proved to be true. In mathematics, by theorems, we generally refer to statements that are of some importance. Less important statements are often called propositions. Axioms are statements that we assume to be true, these come from how we define things, or from our observation of intuition about the world. For example, an axiom can be that "two sets are equal if they have the same elements" (this is known as the Axiom of extensionality in Zermelo-Fraenkel set theory). A less important theorem that is helpful in the proof of other results is called a lemma. A corollary is a theorem that can be established directly from a theorem that has been proved. A conjecture is a statement that is being proposed to be a true statement, but we don't have a proof yet. Now we look at some proof techniques. These are general ideas our proofs usually follow. In writing a proof we have to be creative, we don't have a method or an algorithm to construct a proof for any statement, so we need to be very creative with our arguments. Ideally, a mathematical proof should be elegant and concise, the more simple and short the argument for a complex theorem the more beautiful the proof is.

Direct Proof

The first proof technique we look at is direct proof. Direct proofs are pretty straightforward. A direct proof shows that a conditional statement $p \implies q$ is true by showing that if p is true, then q must also be true so that the combination p true and q false never occurs. We do this by assuming that p is true and use axioms, definitions, and previously proven theorems, together with rules of inference, to show that q must also be true.
We will now look at an example of a direct proof.

Theorem 1. *If n is an odd integer, then n^2 is odd.*

Proof. Let n be an odd integer, then there exists an integer k such that $n = 2k + 1$ (an odd integer is always of form $n = 2k + 1$). Then $n^2 = (2k + 1)^2 = 4k^2 + 2k + 1 = 2(2k^2 + k) + 1$, therefore n^2 is also odd. □

Contrapositive

Often we are unable to prove a statement by direct proof, and for that, we might sometimes use another proof technique called proof by contradiction. Proofs by contraposition make use of the fact that $p \implies q$ is equivalent to its contrapositive, $\neq q \implies \neg p$. This means that $p \implies q$ can be proved by showing that its contrapositive, $\neq q \implies \neg p$, is true. In a proof by contraposition of $p \implies q$, we take $\neg q$ as a premise, and using axioms, definitions, and previously proven theorems, together with rules of inference, we show that $\neg p$ must follow. We will now look at an example of a proof by contrapositive.

Theorem 2. *If $x^2 - 6x + 5$ is even, then x is odd.*

Proof. Let p be '$x^2 - 6x + 5$ is even' and let q be 'x is odd'. Then by the statement $p \implies q$ the contrapositive is, $\neg q \implies \neg p$. Therefore, if x is even, $x^2 - 6x + 5$ is odd. Then x can be represented as $x = 2k$ where $k \in \mathbb{Z}$. Then $x^2 - 6x + 5 = (2k)^2 - 6(2k) + 5 = 4k^2 - 12k + 5 = 2(2k^2 - 6k) + 5 = 2\alpha + 5$ where $\alpha = 2k^2 - 6k$. Then 2α is also an even number as it is of the form $2k$, and since the sum of an even number and an odd number is odd (5 is odd), therefore, the result is odd. □

Contradiction

Often even a proof by contrapositive doesn't work, and we are unsuccessful in proving a statement by contrapositive, in that case, we may also try a proof by contradiction approach. Suppose we want to prove that a statement p is true. Furthermore, suppose that we can find a contradiction q such that $\neg p \implies q$ is true. Because q is false, but $\neg p \implies q$ is true, we can conclude that $\neg p$ is false, which means that p is true. This type of proof is called a proof by contradiction. We will now look at an example of a proof by contradiction.

Theorem 3. *Show that $\sqrt{2}$ is an irrational number.*

Proof. We want to reach a contradiction, and for that, we suppose that the negation of our statement is true. So suppose $\sqrt{2}$ is a rational number. Let $\sqrt{2} = \frac{p}{q}$ for some integers p and q such that $q \neq 0$, also suppose that $\frac{p}{q}$ is in the in lowest terms so $\gcd(p, q) = 1$. Then $2 = \frac{p^2}{q^2} \iff 2q^2 = p^2$ which implies p^2 is even, and therefore p is even. As p is even there exists an integer k such that $p = 2k$. So $2 = \frac{p^2}{q^2} = \frac{(2k)^2}{q^2} \iff q^2 = \frac{4k^2}{2} = 2k^2$, which implies that q^2 is even and so q is even. But if p and q are both even then $\frac{p}{q}$ is not in lowest terms as then $2|p$ and $2|q$ and so $\gcd(p, q) \geq 2$, which is a contradiction as we have that $\gcd(p, q) = 1$. Therefore $\sqrt{2}$ cannot be written in the form $\frac{p}{q}$, and so $\sqrt{2}$ is not rational and therefore $\sqrt{2}$ is irrational. □

Induction

Now we look at another proof technique, called proof by induction. This technique is a bit different from the other proof techniques we have seen so far. Proof by induction uses the principle of mathematical induction. The principle of mathematical induction is used to prove properties regarding the set of natural numbers (or a subset of it) the principle can be generalized to apply to any wellfounded set but at this level, we need not be concerned about that. The principle of mathematical induction is defined as follows, suppose we want to prove $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, then if we show that $P(1)$ is true (this is called the base case), and for any positive integer k, $P(k) \implies P(k+1)$ (this is called the induction step), then we can conclude that $P(k)$ holds for all positive integers. We can think of this like a series of dominoes, if the first domino falls and we have that if any k^{th} domino falling means that $k+1$ domino will also fall then we have that all the dominoes will fall. Now we show an example of proof by induction.

Theorem 4. *For any positive integer n, the sum $1 + 2 + \cdots + n = \sum\limits_{i=1}^{n} i = \frac{n(n+1)}{2}$.*

Proof. By mathematical induction, we show that for any positive integer n, $\sum\limits_{i=1}^{n} i = \frac{n(n+1)}{2}$ holds true.

Base case: $n = 1$

For $n = 1$ we have that $\sum\limits_{i=1}^{1} i = 1$ and $\frac{1(1+1)}{2} = 1$ so this case holds true.

Induction hypothesis: Suppose that $n = k$, $\sum\limits_{i=1}^{k} i = \frac{k(k+1)}{2}$ is true.

Induction step: We use our induction hypothesis to show that $P(k) \implies P(k+1)$.

For $n = k+1$, we want to show that $\sum\limits_{i=1}^{k+1} i = \frac{(k+1)((k+1)+1)}{2}$. We have that $\sum\limits_{i=1}^{k+1} i = \left(\sum\limits_{i=1}^{k} i\right) + k + 1$.

From our induction hypothesis, we have that $\sum\limits_{i=1}^{k} i = \frac{k(k+1)}{2}$, so

$$\sum_{i=1}^{k+1} i = \left(\sum_{i=1}^{k} i\right) + k + 1 = \frac{k(k+1)}{2} + k + 1 = \frac{k(k+1) + 2(k+1)}{2} = \frac{(k+1)(k+2)}{2} = \frac{(k+1)((k+1)+1)}{2}$$

And as $P(k) \implies P(k+1)$, we have that by the principle of mathematical induction for any positive integer n, the sum $1 + 2 + \cdots + n = \sum\limits_{i=1}^{n} i = \frac{n(n+1)}{2}$. □

Problems

1. 1

Give a direct proof that if m and n are both perfect squares, then nm is also a perfect square.

Solution: Let n and m be perfect squares, then there exists integer a and b such that $n = a^2$ and $m = b^2$. So $nm = a^2b^2 = (aa)(bb) = (ab)(ab) = (ab)^2$. Therefore nm is also a perfect square.

□

2. 2

Given that p is a prime and $p|a^n$, prove that $p^n|a^n$.

Solution: As $p|a^n$ then $a^n = kp$ for some integer k.
Case 1: $p \neq a$
Then a is not a prime, then $a = p_1 \times p_2 \times ...p_m$
$a^n = p_1^n \times p_2^n \times ...p_m^n = kp$
As $p|a^n$ and $a^n = p_1^n \times p_2^n \times ...p_m^n$ then there must be some p_i from $1 \leq i \leq m$ such that $p|p_i$
As p_i is prime for all $i \leq i \leq m$, then if $p|p_i$ then $p_i = p$ which means $p|a$
Then $a = pq$ so $a^n = p^nq^n$ therefore $p^n|a^n$.
Case 2: $p = a$
If $p = a$ and $p|a^n$ then as $a^n|a^n$ and $a^n = p^n$ then $p^n|a^n$.

□

3. 3

Show that any composite three-digit number must have a prime factor less than or equal to 31.

Solution: The largest composite three-digit number is 999. Any composite number can be expressed as the product of two or more primes. For a three-digit composite number, the primes must be at most the square root of the number. Therefore, to show that any composite three-digit number must have a prime factor less than or equal to 31, it suffices to show that there are no primes greater than 31 that divide any of the numbers from 100 to 999. Then $31^2 = 961$ which is less than 999. Henceforth it suffices. Then any three-digit number that is divisible by a prime greater than 31 would have to be divisible by the next prime number which is 37. $37^2 = 1369$ which is a 4-digit composite number. Hence shown.

□

4. 4

Show that if a is a positive integer and $\sqrt[n]{a}$ is rational, then $\sqrt[n]{a}$ must be an integer.

Solution: Let $a \in \mathbb{Z}^+$, suppose $\sqrt[n]{a}$ is rational, we show that then $\sqrt[n]{a}$ must be an integer.
Let $\sqrt[n]{a} = \frac{p}{q}$, where $p, q \in \mathbb{Z}$ where $q \neq 0$ and $\gcd(p,q) = 1$.

$$\sqrt[n]{a} = \frac{p}{q} \Leftrightarrow a = \frac{p^n}{q^n} \Leftrightarrow aq^n = p^n$$

Now we have that $q^n | p^n$, but as $\gcd(p,q) = 1$ then $\gcd(p^n, q^n) = 1$.
So as only common divider of p^n and q^n is 1 and $q^n | p^n$ then $q^n = 1$
Therefore $a = \frac{p^n}{q^n} = p^n$, so $\sqrt[n]{a} = p$.
Which means $\sqrt[n]{a}$ is an integer.

□

5. 5

Show that there exists irrational numbers a and b such that a^b is rational.

Solution: It is enough to prove this claim through an example that there exist rational numbers a and b such that a^b is rational.

Consider $a = \sqrt{2}$ and $b = \sqrt{2}$. Then a number $c = a^b = \sqrt{2}^{\sqrt{2}}$ where $c \in \mathbb{R}$

Then either c is rational, or c is irrational.

Case 1: c is rational.
If $c = \sqrt{2}^{\sqrt{2}}$ is rational, then we already have our irrational numbers a and b such that a^b is rational.

Case 2: c is irrational.
If $c = \sqrt{2}^{\sqrt{2}}$ is irrational, then let $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$. Then

$$c = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = 2$$

and 2 is rational.

Hence proved that there exists irrational numbers a and b such that a^b is rational.

□

6. 6

Show that there are infinitely many primes. You may like to use the following definition and theorem in your proof.
Definition: A prime number is a Natural number that is only divisible by 1 and itself and has to be divisible by 2 different numbers.
Fundamental Theorem of Arithmetic: Every integer $N > 1$ has a prime factorization, meaning either N is itself prime or can be written as a product of prime numbers.

Solution: Let $s = \{p_0, p_1, p_2, ..., p_n\}$ be set of all primes.
Let $P = p_0 \times p_1 \times p_2 \times ... \times p_n$
Let $q = P + 1$
Case 1:
q is prime, which is not in our set s
Case 2:
if q is not prime, then there exists a prime factor decomposition of q.
Let f be a prime that divides q, then f would be in our set s thus f would divide P too.
As f divides q and P then f divides $q - P$, which is 1
Then f divides 1.
As $f \geq 2$ f cannot divide 1, thus we have a contradiction.

Hence, the new prime number q does not exist in our set but lies outside the set. But we claimed that our set contains all prime numbers. Therefore, there are infinite prime numbers.

□

7. 7

Show that for any positive integer n, $\sum_{i=1}^{n} 2i - 1 = n^2$

8. 8

Show that for any natural number n, $\sum_{i=1}^{n} 2^i = 2^{n+1} - 1$

9. 9

Prove that for all natural numbers $n > 1$, $\sqrt[n]{n}$ is irrational

Solution: Suppose $\sqrt[n]{n}$ is rational for some $n \in \mathbb{N}$
Then there exists integers a and b, such that $\sqrt[n]{n} = \frac{a}{b}$, where $b \neq 0$ and $gcd(a, b) = 1$

$$\sqrt[n]{n} = \frac{a}{b} \Rightarrow n = \frac{a^n}{b^n}$$

$$gcd(a, b) = 1 \Rightarrow gcd(a^n, b^n) = 1$$

As $n \in \mathbb{N}$, then $b^n = 1$, which means $n = a^n$
As $n > 0$ and $b^n = 1$, then $a^n > 0$, which means that $a > 0$
$a \neq 1$, as if $a = 1$ then $n = \frac{a^n}{b^n} = \frac{1}{1} = 1$, but $n > 1$, so $a \geq 2$
We know for all natural numbers n $2^n > n$ (this result is trivial and can be easily proved by mathematical induction).
So $a^n \geq 2^n > n$, which means $n \neq a^n$, there we have a contradiction without original claim that $n = a^n$
Therefore for all natural numbers $n > 1$, $\sqrt[n]{n}$ is irrational

□

10. 10

Show that $\sqrt{p}$ is irrational for any prime number p.

Solution: Suppose $\sqrt{p}$ is rational then $\sqrt{p} = \frac{r}{q}$ where $q \neq 0$ and $gcd(q,r) = 1$

Then $p = \frac{r^2}{q^2}$, so $pq^2 = r^2$

Now as $r^2 = r \times r$ then any number in prime factorization of r^2 would appear an even number of times.

Similiary any number in prime factorization on q^2 appear and even number of times.

So take $q^2 = p_1 \times p_2 \times ...p_n \times p_1 \times p_2 \times ...p_n$

As $p|r^2$ and $q^2|r^2$ then $r^2 = p \times p_1 \times p_2 \times ...p_n \times p_1 \times p_2 \times ...p_n$

Now p is a number that appears in the prime factorization of r^2 an odd number of times.

Here we have a contradiction, therefore $\sqrt{p}$ is irrational.

□

11. 11

For all positive integers a and b show that $\text{gcd}(a,b)\text{lcm}(a,b) = ab$.

Solution: Let $d = \text{gcd}$ for $a, b \in \mathbb{Z}$. Then $\exists p, q \in \mathbb{Z}$ s.t. $a = pd$ and $b = qd$.

Let $m = \frac{ab}{d}$ then $m = aq = pb$. Which means $a|m$ and $b|m$ which means m is a common multiple of a and b.

Now we need to show that m is indeed the least common multiple of a and b.

Let c be a common multiple of a and b, then $c = at = sb$.

From bezout's lemma we know that $\exists x, y \in \mathbb{Z}$ s.t. $d = ax + by$.

We show that $m|c$ which would imply that $m \leq c$.

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = \frac{cax}{ab} + \frac{cby}{ab}$$

$$\frac{cax}{ab} + \frac{cby}{ab} = \frac{cx}{b} + \frac{cy}{a} = \frac{c}{b}x + \frac{c}{a}y$$

$$\frac{c}{m} = \frac{c}{b}x + \frac{c}{a}y = sx + ty$$

As $s, x, t, y \in \mathbb{Z}$ then $sx + ty \in \mathbb{Z}$, which means $m|c$ theefore $m \leq c$.

Which means m is the least common multiple of a and b.

So we have that $dm = \text{gcd}(a,b)\text{lcm}(a,b) = ab$.

□

12. 12

Prove that at a party where there are at least two people, there are two people who know the same number of other people there. Given that everyone at least knows the host.

Solution: Let there be n number of people at the party where $n \in \mathbb{N}$ and $n \geq 2$
Now the maximum number of people a person can know is $n - 1$
The minimum number of people someone can know is 1 (the host).
Now we have n pigeons and $n - 1$ holes, so with the pigeon hole principle at least 1 hole will have more than 1 pigeon.
So assigning the number of people that know that amount of people from 1 to $n - 1$, there would be at least 1 number k where 2 people are assigned.

□