MAT301H5Y

Week 1 Lecture 1: Prerequisite review

Tuesday May 09th, 2023

3-5pm instructed by Marcu-Antone Orsoni

Main topics covered

The main topics covered in this lecture are related to chapter 1 of the course notes which are related to pre-requisites for the course. This includes most topics typically covered in MAT102 such as Induction, strong induction, relations etc. A notational remark in the course is as below

Notational remark

Conventionally in the course, the following notations for common sets are as below:

- $\mathbb{N} = \{1, 2, 3 \dots\}$
- $\mathbb{N}_0 = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3 \dots\}$
- $\mathbb{Z} = \{\cdots - 3, -2, -1, 0, 1, 2, 3 \dots\}$

Induction

Induction covered in the lecture is the same as the ones covered in MAT102. Suppose we have a mathematical statement $P(n)$ that depends on a natural number n. We want to prove this statement is true for all $n \geq n_0$ for some natural n_0. Note that it is fairly common to see $n_0 = 0$ when it comes to induction exercises but it very well could be 10 or any other natural number. The general regular induction procedure is outlined below

Ordinary induction

1. **Verifying the base case**: Proving that the base case of $n = n_0$ for $P(n)$ holds true. In other words, verifying $P(n_0)$ is true.
2. **Proving the induction step**: By assuming that $P(k)$ is true for some arbitrary $k > n_0$, we need to prove that $P(k+1)$ is true. In other words, we need to prove $P(k) \implies P(k+1)$.
3. **Conclusion**: We conclude from (1) and (2) that $P(n)$ holds true for all $n \geq n_0$ as needed.

What is outlined above is regular or sometimes loosely referred to as "weak" induction. The other form of induction is called "strong" or complete induction as covered in MAT102. The steps, for complete induction are outlined below:

Complete induction

1. **Verifying the base case**: Proving that the base case of $n = n_0$ for $P(n)$ holds true. In other words, verifying $P(n_0)$ is true.
2. **Proving the induction step**: By assuming that $P(i)$ is true for all $1 \leq i \leq k$ for some $k > n_0$, we need to prove that $P(k+1)$ is true. In other words, we need to prove $P(i) \forall i \in \mathbb{N}$ where $1 \leq i \leq k \implies P(k+1)$.
3. **Conclusion**: We conclude from (1) and (2) that $P(n)$ holds true for all $n \geq n_0$ as needed.

Note that you may require more than 1 base case for strong induction in some situations.

Divisibility

We also went over divisibility just like in MAT102. A review of the definitions are as below:

Basic divisibility definitions

When it comes to talking about divisibility for some $n, m \in \mathbb{N}$ we usually talk about the following definitions and notations:

- $n|m$ if and only if there exists $k \in \mathbb{N}$ such that $m = nk$. In this case n is considered to be a divisor(or factor) of m
- p is prime if its sole or only divisors are 1 and p. If a number is not prime it is composite. Note that 1 is neither prime nor composite.
- For all n, m there exists $q \in \mathbb{N}$ and $r \in \mathbb{N}_0$ s.t. $m = nq + r$ where $0 \leq r < n$

We covered two interesting properties of prime numbers in class. These notes also consist of the proofs of these two properties.

Proposition

There exist infinitely many prime numbers.

Proof:

For the proof shown in class, we used a contradiction approach. Assume by contradiction that there are finite number of prime numbers. This means we can construct a finite set consisting of prime numbers. Let S be such a set defined as below:

$$S = \{p_1, p_2, p_3 \ldots p_n\}$$

Let p_n be the largest prime in the set for simplicity and without loss of generality. We know that there are still infinitely many numbers and that there exist numbers larger than any of the primes in S. Let us construct a number P as below:

$$P = p_1 p_2 p_3 \ldots p_n + 1 = \prod_{i=1}^{n} p_i + 1 \tag{1}$$

Notice that $P > p_n$ and thus P is not in S, making P a composite number. Since P is a composite, it must be divisible by at least one prime number. Therefore, there exists $p_k \in S$ such that $p_k|P$. We also see that $p_1 p_2 p_3 \ldots p_n = \prod_{i=1}^{n} p_i$ is also composite which contains p_k and thus $p_k | \prod_{i=1} p_i$. We recall from MAT102 that $b|a$ and $b|c \implies b|(\alpha a + \beta c)$ for integers α, β.

We therefore see that $p_k|P - \prod_{i=1}^{n} p_i$. However, we notice from (1) by rearranging the following:

$$P = \prod_{i=1}^{n} p_i + 1 \implies P - \prod_{i=1}^{n} p_i = 1$$

Substituting we get $p_k|P - \prod_{i=1}^{n} p_i \iff p_k|1$. This is clearly not possible as $p_k > 1$ because 1 is not a prime number and so p_k cannot divide 1. Since this is a logical contradiction, the given assumption that we can construct a finite set consisting of all prime numbers is false and thus the given statement is true and there are indeed infinitely many prime numbers.

■

The next topic of primes is not exactly a property but an interesting way to construct n consecutive composite numbers using properties of prime numbers.

Proposition: constructing n consecutive composite numbers

The following set of consecutive numbers are guaranteed to be composite numbers:

$$S = \{(n+2)! + 2, (n+2)! + 3, (n+2)! + 4, \ldots, (n+2)! + n + 1\}$$

Proof

Firstly let $I = \{1, 2, 3 \ldots n\}$, we see directly that $|S| = n$ indeed which is our requirement(having n consecutive numbers). What's not very easy to observe is why $(n+2)! + i$ is composite for all $i \in I$. We can reach this conclusion via step by step analysis.

First, observe that $(n+2)! = 1 \cdot 2 \cdot 3 \ldots (i-1) \cdot i \cdot (i+1) \ldots n \cdot (n+1) \cdot (n+2)$ and thus it is easy to see that $i|(n+2)!$. We also know trivially that $i|i$. Using a fact from a previous proof, we see that $i|((n+2)! + i)$.

This means that i is a divisor of $(n+2)! + i$ for all $i \in I$. This means that 1 and $(n+2)! + i$ are not the only divisors of $(n+2)! + i$ and therefore by definition $(n+2)! + i$ is composite for all $i \in I$.

■

Equivalence relations

We have studied equivalence relations in MAT102, here is a recap of the definition of a relation and equivalence relation. Recall that a cartesian product of two sets A and B defined by $A \times B$ is defined as below:

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

Definition: Relation

A relation R on a set S is a subset of $S \times S$. Sometimes it is denoted that $a \sim b$ if and only if $(a, b) \in R$.

The definition of an equivalence relation is as below

Equivalence relation

An equivalence relation R on S has the following properties:

- **Reflexivity**: $(a, a) \in R$ for all $a \in S$
- **Symmetry**: $(a, b) \in R \implies (b, a) \in R$
- **Transitivity** $(a, b) \in R$ and $(b, c) \in R \implies (a, c) \in R$ for all $a, b, c \in S$

We also have equivalence classes which were covered in class, the definition is as below:

Definition: Equivalence class

An element a of an equivalence relation R on a set S induces a set called an equivalence class denoted by $[a]$ below:

$$[a] = \{b \in S : (a, b) \in R\}$$

Phrased logically, an equivalence class of a is just the set of all elements in S which are related to a. We realize that $[a] = [b]$ for some fixed $a \in S$ and any $b \in [a]$.

It was left as an exercise in class to show that equivalence classes induce a partition on R. That is to say that all equivalence classes of R are disjoint and their union is R. It was also left as an exercise show that following relation on congruence modulo is indeed an equivalence relation:

Exercise: Congruence modulo equivalence relation.

Consider the relation R on $\mathbb{Z}$ such that for any 2 elements $m, n \in \mathbb{Z}$, we say that $m \sim n$ if and only if $m \equiv n \bmod k$ for some $k \in \mathbb{N}$. Show that R is an equivalence relation. Additionally, proceed to show that all the equivalence classes of R can be written as the set below

$$\mathbb{Z}_k = \{[0], [1], \ldots [k-1]\}$$

Remark: $\mathbb{Z}_k$ is just a shorthand representation, what is left to prove is the right hand of the set equality.