MAT246 - Concepts in Abstract Mathematics

Callum Cassidy-Nolan

September 14, 2019

Contents

List of Definitions

List of Theorems

Chapter 1

Lecture 1

1.1 Induction

Note 1

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

Definition 1 (The principle of mathmatical induction)
suppose $S \subseteq \mathbb{N}$
If

- $1 \in S$
- $k + 1 \in S$ *whenever* $k \in S$

Then

$$\boxed{S = \mathbb{N}}$$

The principle of mathmatical induction is simply saying if 1 is in S then $2, 3, \ldots$ is also in S

Example 1.1.1
Prove

$$\forall n \in \mathbb{N}, \underbrace{1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}}_{\chi}$$

Proof.
Let $S = \{n \in \mathbb{N} : \chi \text{ holds } \}$ At this point we don't know what S consists of but we must

show it is $\mathbb{N}$, then we can conclude that the formula holds for all natural numbers. We commence by verifying that $1 \in S$, we have

$$1^2 = \frac{1(1+1)(2+1)}{6}$$

both the right hand side and left hand side are equal to eachother, so the formula holds for 1.

We will now show if $k \in S$ then $k+1 \in S$. We assume that $k \in S$, that is :

$$1^2 + 2^2 + \ldots + k^2 = \frac{k(k+1)(2k+1)}{6}$$

We observe that if we add $k+1$ to both sides of the above equation we get the left hand side, of what we want to prove.

$$\begin{aligned}
1^2 + 2^2 + \ldots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\
&= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\
&= \frac{(k+1)\big(k(2k+1) + 6(k+1)\big)}{6} \\
&= \frac{(k+1)\big(2k^2 + 7k + 6\big)}{6} \\
&= \frac{(k+1)(k+2)(2k+3)}{6} \\
&= \frac{(k+1)\big((k+1)+1\big)\big(2(k+1)+1\big)}{6}
\end{aligned}$$

After working out the right hand side it is the original formula with $k+1$ subbed in. Therefore we have shown that if $k \in S$ then $k+1 \in S$ as wanted, thus by the principle of mathmatical induction

$$S = \mathbb{N}$$

. ■

Definition 2 (Extended principle of mathmatical induction)
This is the same as normal induction, though now we don't have to start with 1. If

- *Let* $n_0 \in \mathbb{N}, n_0 \in S$
- $k \in S \implies k+1 \in S$

Then

$$\boxed{S \supseteq \{n_0, n_0+1, \ldots\}}$$

Observe that S *is only a subset of these numbers as these are the ones that are guarenteed to be in* S*, there may be others.*

Example 1.1.2
Prove for all integers n *greater than or equal to 7 that the following holds:*

$$\underbrace{n! \geq 3^n}_{}\chi$$

Proof.
Let S be the set of all natural numbers that χ holds for. We verify that $7 \in S$

$$\underbrace{7!}_{5040} \geq \underbrace{3^7}_{2187}$$

therefore 7 satisfies χ and so $7 \in S$. Let $k \in \mathbb{N}$, we assume χ holds for k, that is

$$k! \geq 3^k$$

We will prove

$$(k+1)! \geq 3^{k+1}$$

We observe that $(k+1)! = (k+1)k!$, but recall that we assumed that $k! \geq 3^k$ so we have

$$k!(k+1) \geq 3^k(k+1)$$

Recall that $k \geq 7$

$$\begin{aligned} &\geq 3^k 8 \\ &\geq 3^{k+1} \end{aligned}$$

Therefore, we've shown that

$$(k+1)! \geq 3^{k+1}$$

as required, and so

$$S \supseteq \{7, 8, 9, \ldots\}$$

■

Chapter 2

Lecture 2

Definition 3 (Well Ordering Principle)
Every subset of $\mathbb{N}$ other than $\emptyset$ has a smallest element.

2.1 Proof of Induction

Remark 2.1.1
We accepted the Principle of Mathematical Induction, though we should prove it.

Recall, the Principle of Mathematical Induction, suppose $S \subseteq N$, if

- $1 \in S$
- $k+1 \in S$ whnever $k \in S$

then

$$S = \mathbb{N}$$

We'll prove the statement

Proof.
Let $T = \{n \in \mathbb{N} : n \notin S\}$. suppose that $T \neq \emptyset$, therefore by the Well Ordering Principle we know that T has a smallest element, let n_0 be that element. Note that $n_0 \in \mathbb{N}, n_0 \neq 1$ since $1 \in S \therefore 1 \notin T$, therefore $n_0 \geq 2$.
since $n_0 \geq 2$ we know $n_0 - 1 \in \mathbb{N}$ and that $n_0 - 1 \notin T$ since n_0 is the smallest element in T.

$$n_0 - 1 \notin T \implies n_0 - 1 \in S$$

But by property 2, of S we know that if $n_0 \in S$ then $n_0 \in S$, though this is a contradiction as $n_0 \notin S$
Therefore $T = \emptyset$ and $S = \mathbb{N}$ ∎

2.2 Division

Definition 4 (Divides)
for $a, b \in \mathbb{N}$ *we say that* a *divides* b *if there exists a* $c \in \mathbb{N}$ *such that*

$$b = ca$$

And we say

$$a \mid b$$

Remark 2.2.1
$2 \cdot 3.5 = 7$, *though our definition is only for natural numbers, since no* $c \in \mathbb{N}$ *gives* $2 \cdot c = 7$

Definition 5 (Prime)
$p \in \mathbb{N}$ *is* *prime* *if the only divisor of* p *are* 1 *and* p *and* $p \neq 1$

Example

- 7 is prime, since the only divisor is 1 and 7
- 10 is not prime, 2 and 5 divide 10

Theorem 1 (Product of Primes)
for all $n \in \mathbb{N}, n \neq 1$ n *can be written as a product of primes*

Example

- $42 = 2 \cdot 3 \cdot 7$
- $12 = 3 \cdot 2^2$

Definition 6 (Complete Induction)
Let $S \subseteq \mathbb{N}$

- *if* $n_0 \in S$
  - *and* $k+1 \in S$ *when* $n_0, n_0+1, \ldots, k \in S$

  Then
$$S \supseteq \{n_0, n_0+1, \ldots\}$$

We will prove the product of primes theorem

Proof.
Let $S = \{n \in \mathbb{N} : \text{ theorem holds for } n\}$ we will prove

$$S = \mathbb{N}$$

- 2, is prime therefore it is a product of primes and so the Base Case holds.
- We assume if $2, 3, \ldots, k \in S$ then $k+1 \in S$
  - **Case 1**: $k+1$ is prime, then we are done like the base case
  - **Case 2**: $k+1$ is not prime, then there exists an $m \in \mathbb{N}$ such that $1 < m < k+1$ and $m \mid k+1$ by definition this means

    $$k+1 = c \cdot m, \text{ for some } c \in \mathbb{N}$$

    observe that $1 < c < k+1$ since if $c = 1$,$c = k+1$ or if larger we get a contradiction.
    Therefore we can use the Induction Hypothesis on c and m to write thpem both as a product of primes, multiplying them together gives us a new product of primes equal to $k+1$ as required.

Therefore by the principle of complete induction we can say that

$$S \supseteq \{2, 3, \ldots\}$$

though we want to show that $S = \{1, 2, 3, \ldots\}$ observe that 1 is not a product of primes as it is not prime and also not composite, therefore $1 \notin S$ so $S = \{2, 3, \ldots\}$ ■

The intuition behind this proof comes from the fact that if we take a number say 24 it is either prime or not, in this case it is not, and we can write it as $24 = 6 \cdot 4$ then by an inductive argument, we already know that 6 and 4 are already product of primes so we are done. We will show next that in fact this is a unique product.

Chapter 3

Lecture 3

Recall from last lecture we showed that every natural number besides 1 can be written as a product of primes. Thus we have the following

$$\forall n \in \mathbb{N}, n \geq 1 \implies n \text{ is divisible by some prime}$$

Let's call the above α

3.1 There is no largest prime

Proof.
suppose by contradiction p is the largest prime, that is

$$\{2, 3, \ldots, p\}$$

are all the primes. Let $m = (2 \cdot 3 \cdot \cdots \cdot p) + 1$, we note that for any $j \in \{2, 3, \ldots, p\}$ they must not division m as they each of a remainder of 1. We observe that $m \geq 1$ thus by α we know that there exists some $q \in \mathbb{N}$ where q is prime such that

$$q \mid m$$

So then $q \neq 2, 3, \ldots, p$ and so we have found a new prime, which contradicted that we had found all primes, so we get a contradiction, therefore there is no largest prime. ■

Chapter 4

Lecture 4

Theorem 2 (Fundamental Theorem of Arithmetic)
Every natural number other than 1, is a product of primes (proved last lecture) and the primes in the product are unique (including multiplicity) except for the order in which they occur.

Recall given $n \in \mathbb{N}, n \neq 1, n$ is a product of primes that is

$$n = p_1 p_2 \cdots p_{k-1} p_k$$

for example

$$180 = 9 \cdot 10 \cdot 2 = 3^2 5^1 2^2$$

So equivalently we have

$$\forall n \in \mathbb{N}, 1 < n \implies n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where p_i are distinct primes and $\alpha_i \in \mathbb{N}$

We will prove that the prime factorization of any natural number greater than 1 has is unique by contradiction.

Proof.
We commence

- Suppose there are some numbers with two distinct factorizations into primes.
- Let $\mathcal{X}$ be the set of these numbers, observe that $\mathcal{X} \subseteq \mathbb{N}$ thus by the Well Ordering Principle we let n be the smallest such number in $\mathcal{X}$, we have

  $$n = p_1 p_2 \cdots p_{k-1} p_k = q_1 q_2 \cdots q_{l-1} q_l$$

  (Note here we aren't using powers, but we allow for repeated primes, and that p_i, q_j are primes)
- Suppose that the two product of primes share at least one factor, say $p_r = q_r$, then in each product of primes they cancel out and we get that a new smaller number that can be written as a product of primes, though this would cause a contradiction since we assumed n was the smallest such number with this property.
  - Therefore all the p_i are different than the q_j
- Since we know $p_i \neq q_j$ then specifically $p_1 \neq q_1$ if this is true there are two cases either $p_1 \leq q_1$ or $p_1 \geq q_1$.
- **Case 1**: $p_1 < q_1$
  - We note $n = q_1 q_2 \cdots q_{l-1} q_l > p_1 q_2 \cdots q_{l-1} q_l$
  - $p_1 q_2 \cdots q_{l-1} q_l < n \Leftrightarrow 0 < n - p_1 q_2 \cdots q_{l-1} q_l$
  - Note that $p_i, q_j \in \mathbb{N}$ so the product of any of them is also an element of the naturals, and then also $n - p_1 q_2 \cdots q_{l-1} q_l \in \mathbb{N}$.

Why?

- Note that $m < n \implies m$ has a unique factorization into primes , we know
  - $m = p_1 p_2 \cdots p_{k-1} q_k - q_1 q_2 \cdots q_{l-1} q_l = p_1(p_2 \cdots p_{k-1} p_k - q_2 \cdots q_{l-1} q_l)$
  - $m = q_1 q_2 \cdots q_{l-1} q_l - p_1 q_2 \cdots q_{l-1} p_l = (q_2 \cdots q_{l-1} q_l)(q_1 - p_1)$
    - Together

    $$p_1(p_2 \cdots p_{k-1} p_k - q_2 \cdots q_{l-1} q_l) = \underbrace{(q_2 \cdots q_{l-1} q_l)}_{\chi}(q_1 - p_1)$$
- The left hand side of the above tells us that p_1 is a prime factor of m which means it is also a factor of the right hand side.
  - But observe $p_1 \nmid \chi$ since $p_1 \neq q_j$
  - Therefore it must be that $p_1 | (q_1 - p_1)$ this is true if and only if $p_1 \mid q_1$ since q_1 is prime this means that $p_1 = 1$ or $p_1 = q_1$ either of which are contradictions, therefore

What does this contradict?

$\blacksquare$

Techniques Used in this proof

- Here

Definition 7 (Composite)
A natural number c is called composite if

$$c \neq 1 \qquad\qquad c \text{ is not prime}$$

Q: Can we find 20 consecutive composite numbers?
Yes, consider

$$21! + 2, 21! + 3, \ldots, 21! + 21$$

Observe 2 divides the first number, 3, divides the next on until 21, giving us 20 composites
Q: Can we find k consecutive composite numbers?
Yes, using hte same method we have

$$(k + 1)! + 2, (k + 1)! + 3, \ldots, (k + 1)! + k + 1$$

thus we conclude there are arbitrary long stretches of composite numbers.

4.1 Modular Arithmetic

For some intuition, consider military time, if somone tells us it's 15 o clock we know that this is equivalent to 3 o clock, and this will help us represent this type of situation

First we define the integers that is

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$$

Definition 8 (Congruence)
Let $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. if

$$m \mid (a - b)$$

then we say a is congruent to b and we write

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

Example

- Let $m = 12$ (the hours on the clock)
  - it follows that $13 \equiv 1 \pmod{12}$ since $12 \mid (13 - 1)$
  - $14 \equiv 2 \pmod{12}$ and $23 \equiv -1 \pmod{12}$
  - So this shows us in the world of the clock some numbers are the "same"
- $m = 2$
  - We observe
    * $0 \equiv 0 \pmod 2 \Leftrightarrow 2 \mid (0 - 0)$ which is true since we take $c = 0$ in the definition of divisibility.
    * $1 \equiv 1 \pmod 2$
    * $2 \equiv 0 \pmod 2$
    * $3 \equiv 1 \pmod 2$
    * $4 \equiv 0 \pmod 2$
    * $5 \equiv 1 \pmod 2$