# Number Theory

2018A7PS0193P

January 25, 2021

# 1 Fundamentals

## 1.1 Notation

For the rest of this course, the following notation will be followed:

1. $\mathbb{N}$ is the set of natural numbers

2. $\mathbb{Z}$ is the set of integers

3. $\mathbb{W}$ is the set of whole numbers, i.e. $\mathbb{W} = \mathbb{N} \cup \{0\}$

## 1.2 Induction

Often in number theory, we use inductive proofs to prove our arguments. Induction consists of the following steps:

1. Define an induction hypothesis $P(k)$

2. Verify it works for some base case $k = b$. It is possible multiple base cases need to be verified.

3. Assuming $P(k)$ is true, show that it implies that $P(k+1)$ is true

Remember that $P(k)$ is a statement, not a function. You cannot multiply it by some constant or perform any operations on it.

In weak induction (like in the steps given above), we only assume that $P(k)$ is true. However in strong induction, we assume that $P(i)$ is true $\forall i \in [b, k]$, and use this to prove that $P(k+1)$ is true.

## 1.3   Well Ordering Principle

**Theorem 1.1** (Well Ordering Principle)**.** *Every non empty set of non-negative integers has a least element.*

This is not true about negative integers - consider the case of infinite sets, like the set of all integers. There is no well defined least element.

This principle is equivalent to the principle of induction.

### 1.3.1   Proof of Equivalence to Principle of Induction

First, let us prove that WOP $\Rightarrow$ PMI. Let $P(n)$ be a statement that depends on $n \in \mathbb{N}$. Suppose that:

- $P(1)$ is true

- $P(k)$ is true implies $P(k+1)$ is true for all $k \in N$.

We have to show that $P(n)$ is true for all $n \in N$. Let :

$$S = \{n \in \mathbb{N} : P(n) \text{ is true}\}$$

This means we must show that $S = \mathbb{N}$. Let $T := \mathbb{N} \backslash S$, i.e. $T$ is the complement. Let as assume that $S \neq \mathbb{N}$.

By WOP, $T$ has a least element, say $m$. Note that $m \geq 2$ since $1 \in S$. Then, $m - 1 \notin T$ and $m - 1 \in S$. As such, $P(m-1)$ must be true! However, by our initial assumptions, that would mean $P(m)$ is true as well, so $m \in S$. This creates a contradiction, since $m \in T$. Hence, $S = \mathbb{N}$.

## 1.4   Binomial Theorem

**Theorem 1.2** (Binomial Theorem)**.** *Let $x, y \in \mathbb{C}$ and let $n \in \mathbb{N}$, then*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

**Corollary 1.2.1.**

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

**Lemma 1.3** (Pascal's Identity)**.**

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

**Lemma 1.4.**

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n-k}{k} = F_n$$

# 2  The Division Algorithm

**Theorem 2.1.** *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then, there exist unique integers $q$ and $r$ such that $a + b.q = r$, $r \in [0, b)$.*

**Proof:**

Let $S = \{a - bn : n \in Z, a - bn \geq 0\}$. This set is always non-empty:

- If $a \geq 0$, then $a \in S$

- If $a < 0$, then if $n = a$, we have $a - ab \in S$ since $b \geq 1$.

By WOP, $S$ has a least element, say $r$. So, there exists $q \in Z$ such that $r = a - bq$. Since $r \in S$, we have $r \geq 0$.

Suppose $r \geq b$. Then:

$$a - b(q + 1) = a - bq - b = r - b \geq 0$$

$$\Rightarrow a - b(q + 1) \in S$$

$$\Rightarrow r - b \in S$$

However, $r - b < r$, and $r$ is the least element! This gives us a contradiction. So, $r < b$. As such, we have proved the existence of this solution. Now we must prove it's uniqueness. Suppose there exists $p, r, q', r'$, such that:

$$a = bq + r, 0 \leq r < b$$

$$a = bq' + r', 0 \leq r' < b$$

Assume WLOG $q \geq q'$. Now,

$$r' - r = b(q - q')$$

If $q > q'$, then $r' - r \geq b$. However, $r' - r < b$. So, this is a contradiction, and $q' = q$. The solution must be unique.