LECTURE 3

September 11, 2023

1. Mathematical Induction

Recall in the previous lecture, we started to introduce the concept of mathematical induction.

THEOREM 1.1 (Principal of Mathematical Induction). *Let $S(n)$ be a statement about integers. Assume*

- *There exists an integer $k_0 \in \mathbb{Z}$ such that $S(k_0)$ is true.*
- *For any $k \geq k_0$ if $S(k)$ is true, then $S(k+1)$ must also be true.*

Then $S(n)$ must be true for all $n \geq k_0$.

EXAMPLE 1.2. Prove that for all $n \in \mathbb{N}$, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

SOLUTION. We first show that for the base case $n = 1$, the statement is true. On the left side, we have $\sum_{k=1}^{1} k = 1$ and on the right side, we have $\frac{1\cdot(1+1)}{2} = \frac{2}{2} = 1$, so the base case is true. Now assume that for $n \in \mathbb{N}$, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ holds. Then we want to show that for $n+1 \in \mathbb{N}$, $\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}$. On the left side, we have that

$$\begin{aligned}\sum_{k=1}^{n+1} k &= 1 + 2 + 3 + \cdots + n + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}\end{aligned}$$

as desired. Therefore, by mathematical induction, we have shown that $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

THEOREM 1.3 (Second Principal of Mathematical Induction (Strong Induction)). *Let $S(n)$ be a statement about integers and assume the following:*

- *There exists some integer $k_0 \in \mathbb{Z}$ such that $S(k_0)$ is true.*
- *If $k \geq k_0$ is an integer such that $S(k_0)$, $S(k_0+1)$, ..., $S(k)$ are all true, then $S(k+1)$ must also be true.*

Then for all $n \geq k_0$, $S(n)$ is true.

THEOREM 1.4 (Well-Ordering Principle). *Let A be a nonempty subset of $\mathbb{N} = \{1, 2, 3, ...\}$. Then A has a least element, i.e. there exists an $a_0 \in A$ such that for all $a \in A$, $a_0 \leq a$, or $a_0 = \min(A)$.*

REMARK 1.5. $\mathbb{Z}$ does not satisfy the Well-Ordering Principle (Theorem 1.4) since if we take $\mathbb{Z}$ as a subset of itself, it does not have a least element.

PROOF. We will take for granted that 1 is the least element of $\mathbb{N}$. Take $A \subset \mathbb{N}$ and assume that $A \neq \emptyset$. We will prove using cases.

Case 1: Assume that $1 \in A$, then obvious, $1 = \min(A)$.

Case 2: Assume that $1 \notin A$. Assume A has no least element, i.e. for every $a \in A$, there exists an $a_1 \in A$ such that $a_1 < a$. We will perform a clever strong induction (Theorem 1.3) to show that $A = \emptyset$. This would be absurd. The statement $S(n)$ will be "$n \notin A$". We verify the base case for when $n = 1$. Because we are in Case 2, $1 \notin A$, which is true. For the inductive hypothesis, let $k > 1$ such that $1 \notin A$, $2 \notin A$,..., $k \notin A$. Then we want to show that $k + 1 \notin A$. Assume that $k + 1 \in A$ (for contradiction). Since A has no least element, $k + 1$ is not the least element, therefore there is some $a \in A$ with $a < k + 1$, then $1 \leq a \leq k$, but by the inductive hypothesis, $a \notin A$, which is absurd, and therefore, we finished the induction and so $k + 1 \notin A$.

Therefore, by strong induction, for all $n \in \mathbb{N}$ with $n \notin A$, i.e. $A = \emptyset$. This is absurd. □

DEFINITION 1.6. Let $A \subset \mathbb{Z}$ be a nonempty set.

- An integer $k \in \mathbb{Z}$ is said to be a *lower bound* of A if for all $a \in A$, $k \leq a$.
- If there exists a $k \in \mathbb{Z}$ such that k is a lower bound for A, then we say that A is *bounded below*.

EXERCISE 1.7. Let $A \subset \mathbb{Z}$ be a nonempty subset and bounded below. Prove that A has a least element using strong induction.

EXERCISE 1.8. Formulate what it should mean that a subset of $\mathbb{Z}$ is bounded above.

EXERCISE 1.9. Prove that a nonempty subset $A \subset \mathbb{Z}$ and bounded above has a greatest element using strong element.

2. Division

NOTATION 2.1. For $a, b \in \mathbb{Z}$ with $a \neq 0$, we will say *a divides b* and write $a \mid b$ if b is an integer multiple of a, i.e. there exists some integer $k \in \mathbb{Z}$ such that $b = ka$.

EXAMPLE 2.2. For example, we can consider $2 \mid 4$ and $3 \mid 27$, but $3 \nmid 14$.

PROPOSITION 2.3. *If $a, b, c, x, y \in \mathbb{Z}$ with $a \neq 0$, and $a \mid b$ and $a \mid c$, then $a \mid xb + yc$. To see this,* PROOF. Since $a \mid b$, there exists an integer $k \in \mathbb{Z}$ such that $b = ka$. Similarly, since $a \mid c$, there exists an integer $m \in \mathbb{Z}$ such that $c = ma$. Multiplying the first equation by x and multiplying the second equation by y we obtain $xb = xka$ and $yc = yma$ and so adding these two equations together, we obtain

$$xb + yc = xka + yma = (xk + ym)a$$

where $xk + ym \in \mathbb{Z}$ as well, and thus, by definition of divisibility, $a \mid xb + yc$ as desired. $\square$

PROPOSITION 2.4. *If $a, b \in \mathbb{Z}$ with $a, b \neq 0$ such that $a \mid b$, then $|a| \leq |b|$.*

PROOF. Indeed, since $a \mid b$, we have some integer $k \in \mathbb{Z}$ such that $b = ka$ and so $|b| = |k||a|$. But since $b \neq 0$, then $k \neq 0$ and therefore, $|k| \geq 1$, implying that $|b| = |k||a| \geq 1 \cdot |a| = |a|$, as desired. $\square$

THEOREM 2.5 (Division Algorithm). *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists a unique $q, r \in \mathbb{Z}$ such that $0 \leq r < b$ such that $a = qb + r$. We call q the quotient and r the remainder of the division a by b. By unique, we mean that there is exactly one q and one r that will make $a = qb + r$.*

REMARK 2.6. $a \equiv r \bmod b$ since $a - r = qb$.