Integers

We review 3 fundamental ideas

- mathematical induction
- the division algorithm and GCDs
- prime numbers

Induction

Let $P(n)$ be a logical sentence depending on $n \in \mathbb{Z}$.

The <u>Principle of Mathematical Induction</u> states that if, for some $n_0 \in \mathbb{Z}$, both

① $P(n_0)$ is true [Base case]

and

② for every $n \geq n_0$, $P(n) \Rightarrow P(n+1)$ is true, [Inductive step]

then $P(n)$ is true for all $n \geq n_0$.

The **Principle of Strong Mathematical Induction** states that if, for some $n_0 \in \mathbb{Z}$, both

① $P(n_0)$ is true [Base case]

and

② for every $n \geq n_0$,

$$[P(n_0) \wedge P(n_0+1) \wedge \cdots \wedge P(n)] \Rightarrow P(n+1)$$

is true, [Strong inductive step]

then $P(n)$ is true for all integers $n \geq n_0$.

Despite the name, "strong" induction is equivalent to "ordinary" induction!

The Principle of Mathematical Induction is equivalent to the **Well-Ordering Principle**:

If $S \subseteq \mathbb{Z}$ is a non-empty set of integers which is bounded below (i.e. there exists $m \in \mathbb{Z}$ such that $m \leq x$ for all $x \in S$), then S has a least element (i.e., there exists $n_0 \in S$ such that $n_0 \leq x$ for all $x \in S$).

Proof sketch

(Induction $\Rightarrow$ Well-Ordering)

Suppose $S \subseteq \mathbb{Z}$ is bounded below, and let $m \in \mathbb{Z}$ be a lower bound.

Assume that S has no least element. We prove $S = \emptyset$.

Certainly $n \notin S$ for all $n < m$. Now

<u>Base case</u>: If $m \in S$, then m would be the least element in S. Hence, $m \notin S$.

<u>Inductive step</u>: Let $n \geq m$ and suppose none of $m, m+1, \ldots, n$ are in S. Were $n+1$ to be in S, then it would be the least element in S. Hence, $n+1 \notin S$.

This proves $n \notin S$ for all $n \geq m$, so $S = \emptyset$.

(Well-Ordering $\Rightarrow$ Induction)

Let $P(n)$ be a sentence and $n_0 \in \mathbb{Z}$ such that

Base Case: $P(n_0)$ is true

Inductive Step: $P(n) \Rightarrow P(n+1)$ is true for all $n \geq n_0$.

We wish to conclude $P(n)$ is true for all $n \geq n_0$. That is, the set

$$S = \{ n \in \mathbb{Z} \mid n \geq n_0 \text{ and } P(n) \text{ is false} \}$$

is empty.

If not, it is bounded below by n_0, so it contains a least element m_0.

Since $P(n_0)$ is true, $m_0 \neq n_0$. Thus, $m_0 > n_0$. Since m_0 is the least element in S, $m_0 - 1 \notin S$. Thus, $P(m_0 - 1)$ is true. But $P(m_0 - 1) \Rightarrow P(m_0)$ by the inductive step, making $P(m_0)$ true. This contradicts $m_0 \in S$, so $S = \emptyset$. ■

Division algorithm and GCDs

Thm: Let $n, d \in \mathbb{Z}$ with $d \geq 1$. Then there exist unique $q, r \in \mathbb{Z}$ such that

$$n = dq + r \quad \text{and} \quad 0 \leq r \leq d-1.$$

Proof: Math 3345 or see text.

Def: Let $a, b \in \mathbb{Z}$. The greatest common divisor of a and b is a non-negative integer d such that

① $d \mid a$ and $d \mid b$ (d is a common divisor)

and

② For any $d' \in \mathbb{Z}$ such that $d' \mid a$ and $d' \mid b$, we have $d' \mid d$.

Notation: $d = \gcd(a,b)$

Note: You may have seen a version of this def. where $d' \mid d$ in ② is replaced by $d' \leq d$.

These definitions agree unless $a = b = 0$, in which case our definition gives

$$\gcd(0,0) = 0,$$

but the other definition leaves $\gcd(0,0)$ undefined.