Sec. 7 Complete induction

Euclid's Lemma

Next lecture: Section 10.

Division by a Prime

Recap

Principle of Complete Mathematical Induction (PCMI)

Let $P(n)$ be any statement about n. Suppose we have proved that

$$P(1) \text{ is true} \tag{1}$$

and that

$$\text{for each } n \in \mathbb{N}, \text{ if } P(1), \ldots, P(n) \text{ are all true, then } P(n+1) \text{ is true.} \tag{2}$$

Then we may conclude that for each natural number n, $P(n)$ is true.

Proof by Complete Induction (Template)

To prove $(\forall x \in \mathbb{N})P(n)$ using complete induction:

- Declaration: *Let* $P(n)$ *be the sentence* ...
- BASE CASE: $P(1)$ *is true because* ...
- INDUCTIVE STEP: *Let* $n \in \mathbb{N}$ *such that* $P(1), \ldots, P(n)$ *are all true.*
- Conclusion: *Therefore, by complete induction, for each* $n \in \mathbb{N}$, $P(n)$ *is true.*

Example: Division by a Prime

Theorem 1 (Euclid's Lemma)

Let p be a prime number. Then for all integers x and y, if p divides xy, then p divides x or p divides y.

- We have been using this result without proof for a while; see Remark 4.50.
- It can now be proved using complete induction.

Recall : $\boxed{\text{Division Lemma.}}$

Let $d \in \mathbb{N}$. Then for any $x \in \mathbb{Z}$, there exist unique numbers $q \in \mathbb{Z}$ and $r \in \{0, \cdots, d-1\}$ such that

$$x = qd + r.$$

Proof of Euclid's Lemma

$\Pi = \{\text{all prime numbers}\}$

The theorem in symbols: $\underbrace{(\forall p \in \Pi)(\forall y \in \mathbb{Z})}_{\text{pick arbitrary}}(\forall x \in \mathbb{Z}) \underbrace{[\, p \mid xy \Rightarrow p \mid x \vee p \mid y \,]}_{P(x)}$

<u>Proof</u> Let $y \in \mathbb{Z}$. Let $P(x)$ be the sentence

If $p \mid xy$, then $p \mid x$ or $p \mid y$.

We wish to show that for each $x \in \mathbb{Z}$, $P(x)$ is true.

Since $p \mid xy$ iff $p \mid (-x)y$, and $p \mid x$ iff $p \mid (-x)$,

we see that $P(x)$ and $P(-x)$ share the same truth value.

So it suffices to show that for each $x \in \omega$, $P(x)$ is true.

Goal: $(\forall x \in \omega)\, P(x)$

We shall do so using complete induction.

BASE CASE $P(0)$ is true because $p \mid 0$.

IND. STEP Let $x \in \omega$ such that $P(0), \cdots, P(x)$ are all true.

WTS $P(x+1)$ is true. In other words, we WTS that

if $p \mid (x+1)y$, then $p \mid (x+1)$ or $p \mid y$.

Suppose $p \mid (x+1)y$. (We need to show that $p \mid (x+1)$ or $p \mid y$.)

Now either $\underbrace{p \leq x+1}_{\text{Case 1}}$ or $\underbrace{p > x+1}_{\text{Case 2.}}$

Case 1 Suppose $p \le x+1$. Dividing $x+1$ by p, we get

$$x+1 = qp + r$$

where $q \in \mathbb{N}$ and $r \in \{0, \dots, p-1\}$. Note that $0 \le r \le p-1 \le x$.

Now $ry = \underbrace{(x+1)y}_{\text{divible by } p \text{ by assumption}} - \underbrace{qpy}_{\text{divible by } p.}$ and so $p \mid ry$.

So, by the hypothesis, $p \mid r$ or $p \mid y$.

$$P(x): \quad p \mid xy \Rightarrow p \mid x \vee p \mid y$$

$$P(-x): \quad p \mid (-x)y \Rightarrow p \mid (-x) \vee p \mid y$$

$$P(0): \quad p \mid 0 \cdot y \Rightarrow \underbrace{\overset{T}{p \mid 0} \text{ or } \overset{\text{don't know}}{p \mid y}}_{T} \quad : T$$

$$\underset{T}{(p \mid 0)}$$