453 Lecture 4

1. Well ordering property of the set of natural numbers.

We will accept this statement as an axiom.

"Every non-empty subset of $\mathbb{N}$ has a smallest element."

2. As applications of the well-ordering property we prove the following theorem on Euclidean division.

Thm Given $a, b \in \mathbb{Z}$, $b > 0$, there exists a unique pair of integers q, r satisfying

(i) $a = bq + r$

(ii) $0 \leq r < b$.

Pf: Let $S = \{ a - bq \mid q \in \mathbb{Z},\ a - bq \geq 0 \}$.

We first prove that S is not empty.

If $a \geq 0$ then $a - b(-1)$ is > 0 and belongs to S.

If $a < 0$ then $a - ba = a(1-b) \geq 0$ and belongs to S.

Now using the well ordering property let r be the smallest element of S.

(cont.)

Let $r = a - bq$.
In order to prove property (ii), suppose for the sake of contradiction that $r \geq b$.

Then $r - b \geq 0$ and $r - b < r$.
But $r - b = (a - bq) - b = a - b(q+1)$
Hence, $0 \leq r - b < r$ and $r - b \in S$. This contradicts the choice of r as the smallest element of S!

To prove uniqueness suppose (q_1, r_1), (q_2, r_2) both satisfy (i) and (ii).
Suppose without loss of generality that

$$r_1 \geq r_2.$$

By (i) $\quad a = bq_1 - r_1$
$\quad\quad\quad = bq_2 - r_2$

Subtracting we get

$$0 = b(q_1 - q_2) - (r_1 - r_2)$$

or $\quad r_1 - r_2 = b(q_1 - q_2)$.

But since $0 \leq r_1 < b$ and $0 \leq r_2 \leq r_1$
$0 \leq r_1 - r_2 < b$. But $b \mid r_1 - r_2$. This is only possible if $r_1 - r_2 = 0$. This implies $r_1 = r_2$, which implies $q_1 - q_2 = 0$ (since $b > 0$).
Hence, $r_1 = r_2$, and $q_1 = q_2$. $\blacksquare$