MA 274: Well-Ordering Principle

Theorem (Well-Ordering Principle)**.** If $S \subset \mathbb{N}$ is non-empty, then there is a least element $s \in S$. That is, there exists $s \in S$ such that for all $x \in S$, $s \leq x$.

We apply this to prove the Chinese Remainder Theorem.

Theorem (Chinese Remainder Theorem)**.** Let $a, b \in \mathbb{N}$. Then there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.

Proof. We start by proving the existence of q and r. Let

$$S = \{r' \in \mathbb{Z} : \exists k \in \mathbb{N} \cup \{0\} \text{ s.t } r' = a - bk \geq 0\}.$$

Note that by the definition of S, we have $S \subset \mathbb{N} \cup \{0\}$. In the definition, if we choose $k = 0$, we would have $r' = a \in \mathbb{N}$. Thus, $a \in S$ and $S \neq \varnothing$.

Case 1: $0 \in S$ In this case, there exists $q \in \mathbb{N}$ such that $a = bq + 0$. Since $r = 0 < b$, we have the q and r we were looking for.

Case 2: $0 \notin S$.

Since $0 \notin S$, we have $S \subset \mathbb{N}$. Since $S \neq \varnothing$, by the well-ordering principle, S has a least element $r = a - bq$ for some $q \in \mathbb{N} \cup \{0\}$. Hence $a = bq + r$ and $r \geq 0$. To finish the existence portion of the theorem, we need only explain why $r < b$. We do this by contradiction.

If $r \geq b$, then

$$b \leq r = a - bq$$

Hence, $0 \leq a - b(q+1)$. Let $r' = a - b(q+1)$. Since $r' \geq 0$, the number $r' \in S$. Clearly, $r' < r$, since we are subtracting an additional copy of $b \in \mathbb{N}$. But this contradicts the choice of r to be the *least element* of S. This contradiction implies $r < b$.

Thus, there exists $q, r \in \mathbb{N} \cup \{0\}$ so that $a = bq + r$ and $0 \leq r < b$, as desired. We now show that they are unique.

Suppose, now that there exist q_1, q_2, r_1, r_2 so that

$$\begin{aligned} a &= bq_1 + r_1 \\ a &= bq_2 + r_2 \end{aligned}$$

and $0 \leq r_1 < b$ and $0 \leq r_2 < b$. Without loss of generality, assume that $r_2 \geq r_1$. Then

$$bq_1 + r_1 = bq_2 + r_2.$$

So,

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

Hence, $r_2 - r_1$ is a multiple of b. However, $r_2 - r_1 \leq r_2 < b$. The only non-negative integer strictly less than b that is a multiple of b is 0 and so $r_2 - r_1 = 0$. This implies that $r_2 = r_1$ and $q_2 = q_1$. $\square$