Division Algorithm Proof Outline

Theorem 1.8 [Division Algorithm (Existence Part)] Let a and b be integers with $b > 0$. Then there exist integers q and r such that

$$a = bq + r \qquad \text{and} \qquad 0 \le r < b.$$

(a) Define the set $S = \{a - bk : k \text{ is an integer and } a - bk \ge 0\}$.

(b) Show that S is a nonempty set.

(c) Let r be the least element of S. (How do you know there is one?) Then $r = a - bq$ for some integer q.

(d) Thus $r \ge 0$. (Why?)

(e) Prove by contradiction that $r < b$. First suppose that $r \ge b$, thus $a - bq \ge b$. Show that this leads to a contradiction.

Theorem 1.9 [Division Algorithm (Uniqueness Part)] The integers q and r given by the Division Algorithm (Existence Part) are unique. That is, if $a = bq + r$ and $a = bq' + r'$ with $0 \le r < b$ and $0 \le r' < b$, then $q = q'$ and $r = r'$.

(a) Suppose that $a = bq + r$ and $a = bq' + r'$ for some integers q, q', r and r' with $0 \le r < b$ and $0 \le r' < b$.

(b) Show that $b(q - q') = r' - r$.

(c) Show that $-b < r' - r < b$.

(d) Show that $r' - r = 0$.

(e) Conclude that $r' = r$ and $q' = q$.