**Theorem** (The Division Algorithm). Let \( n \) and \( m \) be natural numbers. Then there exist integers \( q \) (for quotient) and \( r \) (for remainder) such that

\[
m = nq + r
\]

and \( 0 \leq r \leq n - 1 \). Moreover, if \( q, q' \) and \( r, r' \) are any integers that satisfy

\[
m = nq + r = nq' + r'
\]

with \( 0 \leq r, r' \leq n - 1 \), then \( q = q' \) and \( r = r' \).

1.26 **Theorem.** Prove the existence part of the Division Algorithm.

**Proof.** Let \( n \) and \( m \) be natural numbers. Consider the set \( S \) of all integer multiples of \( n \) that are greater than (but not equal to) \( m \). In set-builder notation this is

\[
S = \{ j \in \mathbb{Z} | jn > m \}.
\]

Note that \( mn \geq m \cdot 1 = m \) for all \( m \) and \( n \). This tells us that \( (m + 1)n > m \) and there are integer multiples of \( n \) that are strictly greater than \( m \). Hence, the set \( S \) is non-empty. Note too that \( S \) consists of integers greater than \( m \), a natural number. So \( S \) is a non-empty set of Natural Numbers. We can apply the WOA to \( S \) to obtain a smallest (or least) element. Let’s call this element \( \ell \).

Since \( \ell \) is in \( S \), we have \( \ell \cdot n > m \). Because \( \ell - 1 < \ell \) and \( \ell \) is the least element of \( S \), we must have \( (\ell - 1) \cdot n \leq m \).

Now to be creative! We know that \( \ell \cdot n \) overshoots \( m \) and that \( (\ell - 1) \cdot n \) is less than or equal to \( m \). To show The Division Algorithm works, we need to find \( q \) and \( r \).

Define \( q = \ell - 1 \). Then \( q \cdot n = (\ell - 1) \cdot n \leq m \). Now define \( r = m - q \cdot n \). This automatically gives us that \( m = n \cdot q + r \). What remains to be shown is that \( r \) has the necessary properties.

Is \( r \) nonnegative? Looking at how we define \( q \) and \( r \), we know that \( m \geq nq \) so \( r = m - nq \geq 0 \) and \( r \) is definitely nonnegative.

Is \( r \) less than \( n \)? Because \( \ell \in S \) we know \( m < n\ell \). We also have \( r = m - nq < n\ell - nq = n(\ell - q) \). Remember that \( q = \ell - 1 \), so \( \ell - q = \ell - (\ell - 1) = 1 \). Putting these pieces together gives

\[
r < n(\ell - q) = n \cdot 1 = n.
\]

So \( 0 \leq r < n \). Because \( r \) and \( n \) are natural numbers, \( r < n \) implies that \( r \) must be less than or equal to \( n - 1 \). So \( 0 \leq r \leq n - 1 \). We have verified the existence of integers \( q \) and \( r \) satisfying all necessary properties. □
1.27 Theorem. Prove the uniqueness part of the Division Algorithm.

Proof. Let \( m \) and \( n \) be given as in the statement of the theorem and suppose that \( m = nq + r = nq' + r' \) for some integers \( q, q', r, r' \) satisfying the properties of the Division Algorithm.

If follows easily that \( nq - nq' = r' - r \). Because \( r' \) and \( r \) each satisfy the Division Algorithm, we must have \( 0 \leq r < n \) and \( 0 \leq r' < n \).

If \( r \neq r' \) then one has to be bigger, either \( r < r' \) or \( r' < r \). (We are setting up a contradiction argument and will eventually show the assumption \( r < r' \) or \( r' < r \) leads to something crazy!)

If \( r < r' \) then \( 0 < r' - r < n - r < n \). But \( r' - r = nq - nq' = n(q - q') \), so \( n| (r' - r) \). To summarize, \( r' - r \) is an integer greater than 0 and less than \( n \) that is divisible by \( n \). This is impossible! An almost identical conclusion occurs if we assume \( r' < r \). We must have made some crazy assumption and the only one that we didn’t know for certain was \( r < r' \) or \( r' < r \). These must be false and therefore we must have \( r = r' \).

So \( r = r' \) and \( nq - nq' = 0 \). Because \( n(q - q') = 0 \) and \( n > 0 \), we must have \( q - q' = 0 \). It then follows that \( q = q' \) and \( r = r' \). \( \square \)

The Division Algorithm actually holds for any two integers \( m \) and \( n \) (not just natural numbers). Try to see why the proof above works only for natural numbers \( m \) and \( n \).

Theorems 1.26 and 1.27 are now “closed” for submission. Do the following instead:

1. Find an online proof of the Division Algorithm. This is the only thing you can look up online!
2. Compare and contrast the proofs given here (both existence and uniqueness) versus the proof that you found online. Discuss ways in which each proof could be improved for an audience of students in a Number Theory course.
3. Your submission should typed, double-spaced, and at least a page but no more than two pages. If you choose to include mathematical symbols in your submission, these can be written by hand.
4. This assignment will be graded on a four point scale and is considered “open”.