Math 302 Theorem Set 1: Divisibility

Math 302: Introduction to Proofs via Number Theory

Instructor: Professor Stephanie Treneer, Stephanie.Treneer@wwu.edu

Theorem 1.1. Let a, b and c be integers. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.

Theorem 1.2. Let a, b and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Theorem 1.3. Let a, b and c be integers. If $a \mid b$, then $a \mid bc$.

Theorem 1.4. Let a and b be integers. If $a \mid b$, then for every natural number k, $a^k \mid b^k$.

Division Algorithm. Let a and b be integers with $b > 0$. Then there exist unique integers q and r such that

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

Before you prove the Division Algorithm, let's start with the following related theorems. First we see that setting $b = 2$ in the Division Algorithm suggests the following well-known definitions.

Definition. Let n be any integer. If $n = 2k$ for some integer k, we say that n is *even*. If $n = 2k + 1$ for some integer k, we say that n is *odd*. (Note that these are the only two possibilities when dividing n by 2.)

Theorem 1.5. The sum of two odd numbers is even, and the sum of two even numbers is even, but the sum of an odd number and an even number is odd.

Theorem 1.6. The product of two odd numbers is odd, and the product of two even numbers is even. (Can you prove any more about the product of two even numbers?)

Theorem 1.7. The square of an odd number can be written in the form $8k + 1$ for some integer k.

Now you should prove the Division Algorithm. We'll split it up into two parts:

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

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

Theorem 1.9 (Division Algorithm (Uniqueness Part))**.** ($\star$) 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 $0 \leq r < b$ and $0 \leq r' < b$, then $q = q'$ and $r = r'$.