Math 300 Introduction to Mathematical Reasoning Autumn 2018

Handout 7: The Division Theorem (CORRECTED AGAIN 10/19/18)

One of the most fundamental theorems about the integers says, roughly, "given any integer and any positive divisor, there's always a uniquely determined quotient and remainder." Here's a precise statement of the theorem.

Theorem 1 (The Division Theorem). *If n is any integer and d is a positive integer, there exist unique integers q and r such that*

$$n = dq + r \quad \textit{and} \quad 0 \le r < d.$$

In this theorem, q is called the ***quotient*** and r is called the ***remainder***.

The division theorem is fundamental to the further study of the integers. It will be used, for example, to prove that every integer is odd or even but not both (see Corollary 2 below), and to reduce some theorems about congruences to cases (see Proposition 3.27 in our textbook).

Note that our textbook, and most other math books in the world, call this *the Division Algorithm* for some reason. You should know this name because you'll encounter it in books; but since it's not in any sense an algorithm, I prefer to call it "the division theorem." There are plenty of actual division algorithms available, such as the "long division algorithm" that you probably learned in elementary school.

Also, note that while the textbook states the division theorem (see p. 143), it does not prove it; instead, the author writes, "in this text, we will treat the Division Algorithm as an axiom of the integers." But with our carefully constructed system of axioms, we do indeed have the tools to prove it, and we do so now. This proof is admittedly somewhat more complicated than the ones we have done so far, but it is certainly not beyond our scope, and the work that goes into it is justified by the fundamental importance of this theorem.

Proof of the Division Theorem. Let n be any integer and let d be a positive integer. This is an existence and uniqueness theorem, so we first prove existence, and then prove uniqueness.

To prove existence, we will treat three cases: Case 1 is when n is divisible by d; Case 2 is when n is positive and not divisible by d; and Case 3 is when n is negative and not divisible by d. (Why does this cover all possible cases?)

Case 1 is easy: If n is divisible by d, this means there is an integer q such that $n = dq$, and then the existence statement is verified with this value of q and $r = 0$.

So consider Case 2: Suppose n is positive and not divisible by d. Define a set S of positive integers as follows:

$$S = \{m \in \mathbb{Z}^+ : m \equiv n \pmod{d}\}.$$

Then S is, by definition, a subset of the positive integers. It is nonempty, because n itself is a positive integer congruent to n mod d, so n is an element of S.

The Well-Ordering Axiom (Axiom 12 on the Axioms list) implies that S contains a smallest element: Let's call it r. The fact that $r \in S$ means that r is a positive integer congruent to n mod d, which means in turn that there is an integer q that satisfies $n-r = dq$. We have now produced our integers r and q.

To show that they satisfy the required conditions, we have to verify that $n = dq + r$, $0 \leq r$, and $r < d$. The first statement follows immediately from $n - r = dq$ and algebra, and the second follows from the fact that r is a positive integer.

The only thing left to prove is that $r < d$. This is where we have to use the fact that r is the *smallest* element of the set S. Assume for the sake of contradiction that $r \geq d$. Then there are two possible cases: $r = d$ or $r > d$. If $r = d$, then $n = dq + r = dq + d = d(q + 1)$, which contradicts the assumption that n is not divisible by d. On the other hand, if $r > d$, let r_1 denote the number $r - d$. The fact that $r > d$ implies $r_1 > 0$. Moreover, by algebra,

$$n - r_1 = (dq + r) - (r - d) = dq + d = d(q + 1),$$

which shows that $r_1 \equiv n \pmod{d}$. In other words, we have shown that r_1 is a positive integer congruent to n modulo d, so it is an element of the set S; since it is strictly less than r, this contradicts the fact that r is the smallest element of S. This shows our assumption was false, and therefore $r < d$. This completes the proof of existence in Case 2.

Now consider Case 3: n is not divisible by d and $n < 0$. In this case, we can apply the argument of Case 2 to the positive number $-n$, and obtain integers q_0 and r_0 such that $-n = dq_0 + r_0$ and $0 \leq r_0 < d$. Multiplying the first equation by -1 yields

$$n = -dq_0 - r_0. \tag{1}$$

Note also that the assumption that n is not divisible by d implies r_0 can't be zero, so in fact $0 < r_0 < d$.

In order to find the r and d to satisfy the conclusion, we have to make some adjustments. Let

$$\begin{aligned} q &= -q_0 - 1, \\ r &= -r_0 + d. \end{aligned}$$

As before, we need to show that $n = dq + r$ and $0 \leq r < d$.

To prove the first statement, just note that by algebra we have $q_0 = -q - 1$ and $r_0 = -r + d$. Substituting these equations into (1) yields

$$n = -d(-q - 1) - (-r + d) = dq + d + r - d = dq + r,$$

as desired. For the second statement, we can start with the pair of inequalities $0 < r_0 < d$, multiply through by -1 (changing the direction of the inequalities) to obtain

$$0 > -r_0 > -d,$$

and then add d to all three expressions to obtain

$$d > -r_0 + d > 0,$$

which is the same as $0 < r < d$.

Now that we've completed the proof of existence, we have to prove uniqueness: In other words, if we find two such pairs, they must be equal. To do so, suppose q_1, r_1, q_2, r_2 are all integers satisfying

$$\begin{aligned} n = dq_1 + r_1, \quad 0 \leq r_1 < d, \\ n = dq_2 + r_2, \quad 0 \leq r_2 < d. \end{aligned} \tag{2}$$

Focus on the four inequalities in the right hand column (two with $\leq$ and two with $<$). Let's rearrange these four inequalities, and multiply the ones involving r_2 by -1, to obtain

$$\begin{array}{rr} 0 \leq r_1 & r_1 < d, \\ -d < -r_2 & -r_2 \leq 0. \end{array}$$

Now add these two pairs of inequalities (using Theorems 48 and 49 from the Axioms list) to obtain

$$-d < r_1 - r_2 \quad \text{and} \quad r_1 - r_2 < d. \tag{3}$$

On the other hand, from the equations in the first column of (2), we can conclude that $dq_1 + r_1 = dq_2 + r_2$, and therefore

$$r_1 - r_2 = dq_2 - dq_1 = d(q_2 - q_1). \tag{4}$$

Subsituting this into relation (3), we get

$$-d < d(q_2 - q_1) < d,$$

and dividing through by d (which is positive) yields

$$-1 < q_2 - q_1 < 1.$$

Thus $q_2 - q_1$ is an integer strictly between -1 and 1. Since 0 is the only such integer (how do we know this?), this implies $q_1 = q_2$, and then (4) implies $r_1 = r_2$. □

One of the most useful applications of the division theorem is to answer a basic question about even and odd numbers. An integer n is said to be ***even*** if there exists an integer q such that $n = 2q$, and ***odd*** if there exists an integer q such that $n = 2q + 1$ (see p. 15 in our textbook). One fact that you probably believe to be true is that every integer is either even or odd, but not both. But proving that fact would be very difficult without the division theorem. With it, the proof is easy.

This next result is labeled a "Corollary," which is a name used for a result that is logically the same as a theorem (a statement to be proved from the axioms and preceding theorems), but follows very easily from some recent theorem.

Corollary 2. *Every integer is even or odd, but not both.*

Proof. Suppose n is an integer. By the division theorem, there are unique integers q and r, with $0 \leq r < 2$, such that $n = 2q + r$. There are two cases: Either $r = 0$ or not. If $r = 0$, then $n = 2q$, which is even. If $r \neq 0$, then r is an integer such that $0 < r < 2$. It follows from Theorem 93 on the Axiom list that $1 \leq r \leq 1$ (do you see why?), and therefore $r = 1$. Thus n is odd.

To show that n cannot be both even and odd, suppose for the sake of contradiction that it is both. Then there is an integer q_1 such that $n = 2q_1$, and there is another integer q_2 such that $n = 2q_2 + 1$. We can rewrite these equations as $n = 2q_1 + r_1$ and $n = 2q_2 + r_2$, with $r_1 = 0$ and $r_2 = 1$, and this contradicts the uniqueness assertion in the division theorem. □