## The Division Algorithm

The Division Algorithm is a theorem about the behavior of division among integers. It essentially says that any integer can be divided by a positive integer to get a quotient and a non-negative remainder which is smaller than the number we are dividing by.

We have used this statement implicitly in proofs of statements like the following:

If an integer $a$ is not divisible by 5, then $a^2$ is not divisible by 5

when we said that if an integer $a$ is not divisible by 5 then it must have a remainder of 1, 2, 3 or 4 after division by 5. Sounds obvious? Lets take a closer look at the general statement.

**Theorem. (Division Algorithm)** Let $d \in \mathbb{N}$ and $a \in \mathbb{Z}$. Then there exists unique integers $q, r \in \mathbb{Z}$ such that

$$a \;=\; qd + r$$

where $0 \leq r < d$.

The statement of this theorem is really a doubly quantified statement

$$(\forall d \in \mathbb{N})(\forall a \in \mathbb{Z})(\exists! q \in \mathbb{Z})(\exists! r \in \mathbb{Z})((a = qd + r) \wedge (0 \leq r < d))$$

The exclamation marks after the $\exists$ symbols denote uniqueness, and so $\exists!$ is read "there exists a unique."
Hmmm, this is a little more daunting than the informal statement in the introductory paragraph. Let's see what this looks like with one less quantifier.

**Theorem. (Division Algorithm for division by 5)** Let $a \in \mathbb{Z}$. Then there exists unique integers $q, r \in \mathbb{Z}$ such that

$$a \;=\; 5q + r$$

where $0 \leq r < 5$.

Expressed in logical notation

$$(\forall a \in \mathbb{Z})(\exists! q \in \mathbb{Z})(\exists! r \in \mathbb{Z})((a = 5q + r) \wedge (0 \leq r < 5)).$$

**Much ado about nothing.**
Let's just focus on the existence portion of the theorem. We'll deal with uniqueness later.

Now it may seem "obvious" to you again. After all if I hand you the number 63, you go to the multiple of 5 "just to the left of that" on the number line (a.k.a. 60) and write

$$63 \;=\; 60 + 3 \;=\; 5(12) + 3$$

and you have proven the (existence portion of the) division by 5 version of the Divison Algorithm (DA) for the input 63; $q = 12$ and $r = 3$ satisfies $0 \leq 3 < 5$. I am happy with this answer.

We are cooking with gas here. Let's try a negative number input. If I hand you the number -38, you will still go to the multiple of 5 "just to the left of that" on the number line (a.k.a. -40) and write

$$-38 \;=\; -40 + 2 \;=\; 5(-8) + 2$$

and you have proven the (existence portion of the) division by 5 version of the DA for the input -38; $q = -8$ and $r = 2$ satisfies $0 \leq 2 < 5$. I am impressed and convinced by this reasoning.

Now you say: *It is "obvious" that I can always look to "the multiple of 5 just to the left of a." After all the multiples of 5 appear periodically (with period 5) along the integer number line. Therefore, any integer a will either be a multiple of 5 ($r = 0$ in this case) or there will be a multiple of 5 "just to the left of" a which is "distance" at most 4 away. Isn't this special case of DA "obviously" true? Isn't this a proof? Work with me here Prof Brady...* :-)

**Pleased to meet you. Hope you guess my name.**
OK meet Zoig from the planet PSR B1620-26 b. Zoig has an understanding of our arithmetic, but is not familiar with our ideas of patterns or periodicity. Please convince Zoig of the division by 5 version of the DA theorem.

You: *Hi Zoig. I hope you accept that the division by 5 version of DA is true for* $a = 63$. *After all* $63 = 5(12) + 3$ *and* $0 \leq 3 < 5$.

Zoig: *Hi earth student. Yes, that calculation is correct. I believe that the theorem is true for* $a = 63$. *But you haven't said anything else about other values of a. What about* $a = -38$*?*

You: *Well Zoig, it is true for* $a = -38$ *too.* $-38 = 5(-8) + 2$ *and* $0 \leq 2 < 5$.

*Look, this is generally true. The multiples of 5 repeat periodically with period 5 in the integers. If you hand me any integer, either it is a multiple of 5 or it is at most 4 away from the multiple of 5 just to the left of it on the number line.*

Zoig: *I agree that the calculation is correct and that the theorem is true for* $a = -38$. *However what is this "periodically" of which you speak? How can you claim that something is true for all of the infinitely many integers? Forgive me if this appears rude, but you are a mere carbon-based life form with an expected lifespan of approximately 80 odd earth years. This is a child's lifetime for our species; yet even we would not be so presumptuous as to claim that infinitely many statements are true on the basis of two examples.*

You: *Really?! I can't fathom how you guys ever achieved interstellar space travel!*

Zoig: *$&%#!!!*

Zoig may be the ultimate devil's advocate, but makes a good argument. You should concede the following point that Zoig is making. The statements

$$(63 = 5(12) + 3) \wedge (0 \leq 3 < 5)$$

and

$$(\forall a \in \mathbb{Z})(\exists! q \in \mathbb{Z})(\exists! r \in \mathbb{Z})((a = 5q + r) \wedge (0 \leq r < 5))$$

are very, very different. The latter (ignoring the uniqueness components) asserts the existence of **infinitely many** statements of the former type, one for every integer $a$. You are a finite creature with limited time on this earth, and will never check all cases explicitly. Even when you make claims about periodicity: if you are honest, you probably imagine the number line with numbers listed in finite space (in your imagination). But the integers get so large that writing them out explicitly (in base 10) eventually exceeds your imagination. But the latter statement is quantifying over all these integers, and the general form of the DA is also quantifying over all non-negative integers $d$.

**OK so what's going on?**
I don't want to freak you out. I believe that the division by 5 version of the DA is true. Indeed I believe that the general DA (which is equivalent to infinitely many statements like the division by 5 version of the DA, one for every natural number $d \in \mathbb{N}$) is also true.

However, I do not accept that they "follow from concrete examples" or even that they follow from concrete examples plus some hand waving discussion about "patterns" and "periodicity."

They are universally quantified statements about infinitely many integers, and they only follow mathematically and logically from other statements concerning infinitely many integers. But then you will need some starting point; namely, some universally quantified statement about the integers taken as an axiomatic fact. Enter the Least Principle, also known as the well-ordering axiom for $\mathbb{Z}_{\geq 0}$.

It is good practice to limit the number of axioms that you use in any theory, especially axioms that say something about infinity. But we need some axiomatic starting point if we are to be able to talk sensibly about infinity and results holding true for infinitely many integers etc. So we accept the Least Principle as an axiom, and prove other statements using it. Very famous principles are proven as consequences of the Least Principle. For example, the Principle of Induction, which is the key architecture underlying all of our proofs by induction follows from the Least Principle.

**Least Principle.** Every non-empty subset of $\mathbb{Z}_{\geq 0}$ has a least element.

**Examples.** The even natural numbers have 2 as the least element. The multiples of 10 have 10 as a least element. This is the "obvious sounding statement" that we take as an axiom.

**Theorem. (Division Algorithm for division by 5)** Let $a \in \mathbb{Z}$. Then there exists unique integers $q, r \in \mathbb{Z}$ such that

$$a \ = \ 5q + r$$

where $0 \leq r < 5$.

**Pre-proof comments.** The intuition about locating a multiple of 5 "just to the left of or equal to" $a$ is excellent. We just need to relate this intuition to the Least Principle somehow. One idea is to consider the differences between $a$ and multiples of 5. These differences are integers, and if the multiple of 5 is not to the right of $a$, these differences are in $\mathbb{Z}_{\geq 0}$. The least element of this set of differences will be the difference between $a$ and this multiple of 5 just to the left of or equal to $a$. The existence of this least element is assured by the Least Principle; this in turn establishes the existence of a multiple of 5 equal to or just to the left of $a$.

*Proof (existence only).* Consider the set of non-negative integers

$$S \ = \ \{a - 5m \mid m \in Z, \ a - 5m \geq 0\}.$$

First we prove that the set $S$ is not empty. There are two cases to consider.

- **Case $a \geq 0$.** In this case, if we choose $m = 0$ we see that $a - 5(0) = a \in S$ and so $S$ is not empty.
- **Case $a < 0$.** In this case, if we choose $m = a$ we see that $a - 5a = (-a)(5 - 1) > 0$ because $(-a) > 0$ and $(d - 1) = 4 > 0$. Thus $S$ is not empty.

In either case, $S$ is not empty. By definition of the set $S$ it is a collection of non-negative integers and so is a subset of $\mathbb{Z}_{\geq 0}$. The Least Principle implies that $S$ has a least element. Denote this least element by $s_0$. Let us consider properties of $s_0$.

First, $s_0 = a - 5q$ for some integer $q$, because $s_0$ is an element of $S$. Second, $0 \leq s_0 < 5$. The inequality $0 \leq s_0$ is immediate from the definition of the set $S$. We prove the second inequality by contradiction. Assume to the contrary that $s_0 \geq 5$. Then $s_0 - 5 \geq 0$. But $s_0 - 5 = a - 5q - 5 = a - 5(q + 1)$. These two properties mean that $s_0 - 5 \in S$. But this contradicts the fact that $s_0$ is

the **least element** of $S$. This contradiction arose from the assumption that $s_0 \geq 5$. Therefore, this assumption is false, and the inequality $s_0 < 5$ is true.

Taking $r = s_0$, we have proven the existence of two integers $q, r$ such that

$$a \;=\; 5q + r$$

and $0 \leq r < 5$. □

**Remark 1.** Think about the way in which the issue of infinitely many statements about integers $a$ is translated into corresponding statements about sets of differences

**Remark 2.** See the Least Principle handout for the derivation of the general DA (which is a universally quantified version of the division by $d$ version of the DA over $d \in \mathbb{N}$).

**Remark 3.** It is good practice to work yourself into a state about mathematical statements that involve the infinite. For one, you end up learning which statements are "really following" from which other statements. Two, it is dangerous to happily accept universally quantified statements about infinite sets, even if they seem intuitively obvious. One's intuition about the infinite can go awry at times, so it is good to be ever cautious. Three, being uncomfortable about accepting statements about the infinite puts you in excellent company: Euclid was never happy with his "axiom of the parallels" because it stated something about lines "never meeting." Indeed, Euclid was so perturbed by this axiom that he avoided using it in proofs until it was absolutely necessary. For over 2 millennia following Euclid, mathematicians tried to deduce the parallel postulate as a consequences of Euclid's other axioms.:

$$\text{Remaining axioms} \longrightarrow \text{Axiom of Parallels.}$$

We know that this is equivalent to proving the following:

$$\text{Remaining axioms} \wedge \text{negation of Axiom of Parallels} \longrightarrow \text{contradiction.}$$

In the first half of the 19th century mathematicians finally realized that they were never going to obtain a contradiction from assuming "Remaining axioms $\wedge$ negation of Axiom of Parallels." Indeed they were in fact discovering theorems in an entirely new geometry (one that is as logically consistent as the original axiomatic euclidean geometry) called *hyperbolic geometry.* The first published accounts of hyperbolic geometry were due to Nikolai Ivanovich Lobachevsky (in 1829) and independently to Janos Bolyai (in 1831).