Math From Scratch Lesson 14: Division and Remainder

W. Blaine Dowler

May 28, 2011

Contents

1 Defining Division

We can now define the fourth operation taught in most schools in a somewhat familiar way. If a, d, q and r are all integers, then we can find values for them such that

$$a = d \cdot q + r$$

In this representation, we refer to a as the *dividend*, d as the *divisor*, q as the *quotient* and r as the *remainder*.

In fact, we can find several different representations for this which work. For example, if $a = 31$ and $d = 5$, then we can have $q = 6$ with $r = 1$, or $q = 5$ with $r = 6$, or $q = 4$ with $r = 11$, or $q = 1000$ with $r = -4969$. This is where the absolute value comes into play. If we constrain r such that $0 \leq r < |d|$, and we constrain $a \neq 0$ and $d \neq 0$, then the representation will be unique for any given pair of $a \neq 0$ and $d \neq 0$. Note that, if $a = d = 0$, then we can say $r = 0$ and satisfy the above expression with any arbitrary q. The proof that this is unique

for $a \neq 0$ and $d \neq 0$ is what metric spaces and number lines were introduced for at this stage.

Let us examine this in more detail. If a and d are predetermined, then we have the opportunity to find a q which works. We must show that there *is* a q_i such that the corresponding r_i is constrained as $0 \leq r_i < |d|$, and that there is only one such r. The axiom of inequality allows us to define $q_{i+1} = q_i + 1$ with the confidence that no possible q_j such that $q_{i+1} < q_j < q_i + 1$. With this, we must establish two facts:

1. When incrementing q_i to $q_{i+1} = q_i + 1$, then the distance between r_i and r_{i+1} is less than or equal to $|d|$, thereby ensuring that there is at least one value of r such that $0 \leq r < |d|$.
2. We much also show that the distance between r_i and r_{i+1} is greater than or equal to $|d|$, thereby ensuring that only *one* possible value of r satisfies $0 \leq r < |d|$.

This pair of requirements combine to show that we need to prove that the distance between r_i and r_{i+1} is exactly $|d|$. To avoid the nearly inevitable confusion borne of having the same symbol d represent both the divisor and the metric function, we will use the symbol g for our metric function such that

$$g(x, y) = |x - y|$$

Well, if $a = d \cdot q + r$, then $a - d \cdot q = d \cdot q + r - d \cdot q = r$. Let us calculate the following:

$$\begin{aligned}
g(r_i, r_{i+1}) &= g(a - d \cdot q_i, a - d \cdot q_{i+1}) \\
&= |(a - d \cdot q_i) - (a - d \cdot q_{i+1})| \\
&= |a - d \cdot q_i - a + d \cdot q_{i+1}| \\
&= |-d \cdot q_i + d \cdot q_{i+1}| \\
&= |d \cdot (q_{i+1} - q_i)| \\
&= |d \cdot (q_i + 1 - q_i)| \\
&= |d \cdot 1| \\
g(r_i, r_{i+1}) &= |d|
\end{aligned}$$

This is exactly what we needed to prove that our above representation is unique once we constrain our remainder r such that $0 \leq r < |d|$.

Definition The process of *division* is the process of finding values of q and r such that, for a given pair a and d, the equation $a = d \cdot q + r$ is satisfied, where r

is subject to the constraint $0 \leq r < |d|$. We also refer to this process as *dividing a by d*. This can be written mathematically as $a \div d = q \text{ R}r$. In a later lesson, we will see that it can also be written as $\frac{a}{d} = q \text{ R}r$, once we have reached a stage in which fractions can be sensibly defined.

Notice that r has no constraints relative to q. In fact, interchanging d and q can lead to very different values of r. For example, if $a = 6$ and $d = 5$, then $q = 1$ and $r = 1$. However, if instead $a = 6$ and $d = 1$, then $q = 6$ and $r = 0$.

2 The Division Algorithm: Version 1

With this definition, a simple division algorithm presents itself for determining the values of q and r. We examine the combination $a - d \cdot q = r$ as previously defined. For a given a and d, we begin with a particular value of q, say $q_1 = 0$, and compute the corresponding r_1. If $0 \leq r_1 < |d|$, then we are done. If not, and $r_1 < 0$, then we choose $q_2 = q_1 - 1 = -1$, and compute r_2. If $r_1 \geq |d|$, then we choose $q_2 = q_1 + 1 = 1$ and compute r_2. We continue this process until we find our final r_n such that $0 \leq r_n < |d|$ is true.

For example, let $a = 15$ and $d = 4$. Then we choose $q_1 = 0$ and find that $15 - 4 \cdot 0 = r_1 = 15$. As $15 \geq |4|$, we choose $q_2 = 1$ and compute $15 - 4 \cdot 1 = r_2 = 11$. Well, $11 \geq |4|$, so we try $q_3 = 2$ for $15 - 4 \cdot 2 = r_3 = 7 \geq |4|$, which leads to $q_4 = 3$ and $15 - 4 \cdot 3 = r_4 = 3$. As $0 \leq 3 < |4|$, we are now done; we have determined that $15 \div 4 = 3R3$.

For another example, let $a = -9$ and $d = 2$. Again, we begin with $q_1 = 0$ and compute the following succession:

$$\begin{aligned} -9 - 2 \cdot 0 &= -9 < 0 \\ -9 - 2 \cdot (-1) &= -7 < 0 \\ -9 - 2 \cdot (-2) &= -5 < 0 \\ -9 - 2 \cdot (-3) &= -3 < 0 \\ -9 - 2 \cdot (-4) &= -1 < 0 \\ -9 - 2 \cdot (-5) &= 1 \end{aligned}$$

Thus, $-9 \div 2 = -5R1$ as $0 \leq 1 < |2|$.

While this algorithm works, it is clearly far more tedious than the method we learned in grade school. Even the author does not use this method explicitly to calculate something like $14535 \div 127$. However, to find this more efficient method, we must first establish some useful properties of division.

3 Cases of Division With Zero Remainder

In lesson nine, we defined multiples and factors, such that, whenever $a = b \cdot c$ with $a, b, c \in \mathbb{Z}$, we say that a is a multiple of b, a is a multiple of c, b is a factor of a, and c is also a factor of a. (Note that b and c have no special relationship to each other.)

If one replaces the symbols b and c with d and q, we immediately see that this is the case of division with a zero remainder. We write this special case of division as $d|a$, which is read "d divides a." We have also proven that this representation is unique for a given d.[1]

3.1 Properties of Division by Factors

Remember, for all cases in which we have factors ($d|a$) we know that $r = 0$.

1. If $d|a$, then $-d|a$. Given $d|a$, we may assume that there is a q for which $a = d \cdot q$. Well, in lesson ten we proved that $d \cdot q = (-d) \cdot (-q)$, therefore $a = (-d) \cdot (-q)$ is also true. We have no undue restrictions on q, and therefore, if d is a factor of a, then $-d$ is also a factor of a.

2. $a|a$ and $1|a$ for all $a \neq 0$. We show that $a|a$ by choosing $q = 1$, and show that $1|a$ by choosing $q = a$.

3. One cannot divide by 0. We begin by assuming that $d = 0$. Then, r is constrained as $0 \leq r < |d|$, then $0 \leq r < 0$. The left side of that inequality states that r can be as small as 0, but cannot be less than 0. The right side states that r *must* be less than 0. That is a logical inconsistency. Now, we do have the freedom to choose some flexibility in our restrictions on r. In fact, we could restrict r to any interval $a \leq r < b$ provided that $b - a = |d|$ and that[2] $a \leq 0 < b$. We could set our restriction to $-1 \leq r < |d| - 1$ and eliminate the above problem. The problem we then have is that the quotient is no longer unique, and that 0 would be the only number divisible by 0.

   To see this explicitly, look at what happens when setting $d = 0$. For some a, we then have $a = 0 \cdot q + r = r$. However, a is unrestricted, while r is constrained as $-1 \leq r < |d| - 1$. The only possible way to have a logically consistent way to set this up is if we also set $a = r = 0$, simply for the

[1] It may not be unique for *arbitrary* d; we can say that $60 = 6 \cdot 10$ as easily as $60 = 5 \cdot 12$. However, if we arbitrarily choose $a = 60$ and $d = 6$, then $q = 10$ and $r = 0$ are the only possible values which satisfy $a = d \cdot q + r$ with $0 \leq r < |d|$.

[2] This second condition is required solely to retain the idea of factors. We do not, strictly speaking, require this condition, but it allows for numerous interesting possibilities.

purposes of satisfying the equation. However, the equation $0 = 0 \cdot q + 0$ is satisfied for every possible q, so the formulation is not unique.

4. 0 is divisible by everything. Let us examine $0 = d \cdot q + r$. We have the freedom to choose any $d \neq 0$ we like; all we need are a unique combination of q and r to satisfy the system. Well, if $q = r = 0$, then the equation is satisfied regardless of the specific value of d. Note that this is different from the case of division by zero; we require a unique pair of q and r, but only *after* we have chosen our arbitrary $d \neq 0$. The problem previously was that the choice of our arbitrary $d = 0$ did *not* lead to a unique q.

5. If $|d| > |a|$ with $a \neq 0$, then d does not divide a with zero remainder. In fact, when $a > 0$, $a = d \cdot q + r$ is satisfied only with $q = 0$ and $r = a$. For $a < 0$, then the final result depends on d. This is more clear with an explicit example. Let $a = -2$ and $d = 3$. The possible values of r will be 0, 1 and 2. If $q = 0$, then we have $-2 = r$, which is impossible for the allowed values of r. Instead, we must have $q = -1$. This gives us $-2 = -3 + r$, which is satisfied for $r = 1$. Generally speaking, if $a < 0$, $d > 0$ and $|d| > |a|$, then the system is solved with $q = -1$ and $r = d + a$. However, if we have $a < 0$, $d < 0$ and $|d| > |a|$ (changing only the "sign" of d), then the system is solved with $q = 1$ and $r = a - d$. Thus, in these cases, the only way to have zero remainder is if $d + a = 0$ or $a - d = 0$ (as we have specified that $a \neq 0$.) Well, we are only investigating the case in which $|d| > |a|$, which eliminates both $d + a = 0$ and $a - d = 0$.

6. The only factors of 1 and -1 are 1 and -1. This follows immediately from the previous result, as when $|a| = 1$, we have either $|d| > |a|$ or $|d| = |a|$. The previous result eliminates $|d| > |a|$, so that leaves $|d| = |a|$.

4 The Division Algorithm: Version 2

The bases representation theorem introduced in lesson 11 is useful again here. Let us take the explicit example of $14535 \div 127$ to illustrate the algorithm.

The bases representation theorem gives us the equation

$$14535 = 1 \cdot 10^4 + 4 \cdot 10^3 + 5 \cdot 10^2 + 3 \cdot 10 + 5$$

As indicated in property 5 above, 127 cannot divide any single digit number with $q \neq 0$. We are looking for a way to divide efficiently, so the algorithm will be most useful if we can eliminate the greatest number of subtraction steps. This is done by taking the terms $a_i k^i$ with the highest possible values of i into consideration. If we combine the first three of these ($i = 3, 4, 5$) then we have

the following:

$$14535 = 145 \cdot 10^2 + 3 \cdot 10 + 5$$

We have formed 145 by taking the smallest possible combination of the leftmost digits of our dividend 14535 which is greater than or equal to our divisor 127. We then apply our first division algorithm to 145 to obtain

$$14535 = (127 \cdot 1 + 18) \cdot 10^2 + 3 \cdot 10 + 5$$

We can rearrange this to obtain

$$14535 = 127 \cdot 1 \cdot 10^2 + 18 \cdot 10^2 + 3 \cdot 10 + 5 = 127 \cdot 1 \cdot 10^2 + 183 \cdot 10 + 5$$

We apply the division algorithm to the number 183 which appeared here to obtain

$$14535 = 127 \cdot 1 \cdot 10^2 + (127 \cdot 1 + 56) \cdot 10 + 5 = 127 \cdot \left(1 \cdot 10^2 + 1 \cdot 10\right) + 565$$

We divide 565 by 127 to obtain

$$14535 = 127 \cdot \left(1 \cdot 10^2 + 1 \cdot 10\right) + (127 \cdot 4 + 57) = 127 \cdot \left(1 \cdot 10^2 + 1 \cdot 10 + 4\right) + 57$$

which reduces to

$$14535 = 127 \cdot 114 + 57$$

which tells us that $14535 \div 127 = 114R57$.

Although this process is faster and more accurate than counting 114 repeated subtractions, we can still fine tune it somewhat with improved notation. This is the "long division" notation introduced relatively early in traditional mathematics instruction.

We begin with the arrangement of the numbers. We start by writing our divisor, and then putting our dividend under the "long division" symbol as follows:

$$127 \,)\overline{14535}$$

We read the digits of our dividend 14535 from the left, until we identify that it takes 3 digits to form a number greater than our divisor of 127. $145 = 127 \cdot 1 + 18$, so we write the first digit of our quotient (1) above the 5 which would serve as the "ones place" in 145:

$$\begin{array}{r} 1 \\ 127 \,)\overline{14535} \end{array}$$

This step is often performed before breaking down 145 completely as $145 = 127 \cdot 1 + 18$. Rather, we use 1 as our best estimate of that digit in our quotient, and then multiply it by our divisor 127 and writing it below the first three digits of our dividend 14535, and then subtracting to find the "remainder" 18. Had the remainder 18 been a number larger than 127, or had it been negative, we would have been forced to adjust our estimate of that digit of the quotient and try again. The result is the following:

$$\begin{array}{r} 1 \\ 127\,)\overline{14535} \\ \underline{-127} \\ 18 \end{array}$$

We now need to perform the step of combining the remainder 18 with the next digit of our dividend 14535. We "bring down" the 3, writing it next to the digits 18, to form

$$\begin{array}{r} 1 \\ 127\,)\overline{14535} \\ \underline{-127} \\ 183 \end{array}$$

With this, we continue the algorithm, dividing 127 now into the 183 at the bottom of our construction to form

$$\begin{array}{r} 11 \\ 127\,)\overline{14535} \\ \underline{-127} \\ 183 \\ \underline{-127} \\ 56 \end{array}$$

We continue the algorithm for our last digit, recognizing that $565 = 127 \cdot 4 + 57$ to obtain:

$$\begin{array}{r} 114 \\ 127\,)\overline{14535} \\ \underline{-127} \\ 183 \\ \underline{-127} \\ 565 \\ \underline{-508} \\ 57 \end{array}$$

This is long division as it is first learned. It works because the combination of the bases representation theorem and the division $a = d \cdot q + r$ are both unique

representations of the numbers involved.

5 Upcoming Lessons

The next lesson is straightforward but critically important: we'll be dealing with prime numbers, composite numbers, and perfect squares, in a discussion that results in the fundamental theorem of arithmetic.