Math From Scratch Lesson 11: All Your Bases Are Belong To Us

W. Blaine Dowler

December 7, 2010

Contents

1 Writing Numbers

To this point, when working in theory, we have typically not cared about what specific value a number a has had, unless $a = 0$ or $a = 1$. In our examples, we have used other numbers, such as 24.[1] However, we have not yet defined exactly what the symbols "2" and "4" mean when written in this fashion. For example, what exactly is the difference between "24" and "42" in the formal, mathematical sense? That will be the question explored in this lesson.

Theorem 1.1 *The bases representation theorem states that, for any given natural number a, there is a unique representation to base k such that*

$$a = a_m k^m + a_{m-1} k^{m-1} + \ldots + a_2 k^2 + a_1 k^1 + a_0$$

[1]The author also used this notation in lesson 3 when adding numbers via set theory, as writing 15 in set theoretic representation takes up far too much space on the page.

Name	Symbol	Number
Zero	0	
One	1	•
Two	2	••
Three	3	•••
Four	4	••••
Five	5	•••••
Six	6	••••••
Seven	7	•••••••
Eight	8	••••••••
Nine	9	•••••••••

Table 1: The base ten symbols.

such that every $a_i \in \mathbb{W}$*, every* $a_i < k$*, either* $a_i = 0$ *or* $a_i > 0$*, and at least one* $a_i \neq 0$.

Note that, for efficiency, we will combine the two statements $a_i = 0$ and $a_i > 0$ into a single statement $a_i \geq 0$, where the symbol $\geq$ implies that either $>$ or $=$ applies. With this definition, k is our base. While it is intuitive to understand that each number can be represented to a particular base in only one way, it must technically be proven formally.

First, we should choose a base. In the number system adopted through most of the world, we use base ten, because ten is the most common number of fingers that humans are born with. Thus, we will need ten unique symbols to represent the various a_i in our numbers. We define those symbols, along with the number of countable objects they represent, in table 1.

Notice that we do not yet have a symbol for ten. As ten is our base, that may seem odd; this is a somewhat important number. Shouldn't it get its own symbol? No, it doesn't. The symbols are for the values of a_i, which are strictly less than k, which is ten in our representation. What combination of symbols do we use for ten?

By our above definition, ten would be the successor to 9, meaning it is the number one higher than nine. With the a_i representation, ten is given by $1 \cdot k$, where we have omitted all terms for which $a_i = 0$. Keeping the k around gets cumbersome, so we have adopted a particular convention: we identify the value of m such that $k^m \leq a < k^{m+1}$ for our number a. We choose *not* to omit any a_i for which $i \leq m$, even if $a_i = 0$. This appears to have extended our representation to $1 \cdot k + 0$, which is more work. Then we adopt a second convention: we omit the k^i+ pieces of our representation, and simply write a as a string of adjacent numbers, starting with a_m and running down in sequence until we reach a_0. In this case, ten is represented by 10, and is still special as it is the smallest natural number which must be represented by more than one symbol. When these symbols are written in strings in this fashion, they are called *digits*. As we have chosen a particular order to them, each digit has a *place value* representing the value of k^i corresponding to that place in the string. a_0, for example, goes in the ones place, as one is the smallest natural number which fits entirely in that digit of the string. a_1 goes in the tens place, a_2 in the hundreds place, and so on.

So how do we select the values of a_i? Well, we know that $k^m \leq a < k^{m+1}$ for some m. Then, we try each symbol in sequence until we find the value of a_i such that $a_i \cdot k^m \leq a < (a_i + 1)k^m$. Once found, we set $a_i = a_m$. Note the inequality on the left: that is required for cases in which only one a_i is nonzero. To find the next digit, we find the value of a_j such that $a_j \cdot k^{m-1} \leq a - a_m \cdot k^m < (a_j + 1)k^{m-1}$, and continue the process, subtracting the pieces we have already accounted for with each step. This algorithm will find at least one representation of a to base k.

1.1 Proving the Bases Representation Theorem

Now we can prove that the representation defined above is unique. This proof will be less formal than some of our others, given the intuitive nature of the result. The interested and pedantic reader should be able to add the requisite formal details onto the following logic.

We know that we start with $k^m \leq a < k^{m+1}$ to determine the highest power of k to use in our representation. As of lesson 10, we have imposed a rigid order on both $\mathbb{W}$ and $\mathbb{N}$, so we know that the "less than" and "greater than" relations are transitive relations, so we know that this value of m is unique, as equality is only allowed on one side. (i.e. $a = k^m$ is permitted, but $a = k^{m+1}$ is not.) We can use the same logic to show that there is a unique a_i which satisfies $a_i \cdot k^m \leq a < (a_i + 1)k^m$. Thus, we know that a_m is unique. Next, we calculate $a - a_m \cdot k^m$. As the integers numbers are closed under addition and multiplication, and as subtraction is merely adding the additive inverse, we know that $a - a_m \cdot k^m$ is as unique as a_m and k^m. Let us assign $b = a - a_m \cdot k^m$. Now, we can apply the same logic to indicate that the first digit of b is unique; as this will also be the second digit of a, the second digit of a is also unique. We can continue in this fashion, treating each subsequent digit as the maximal digit of some other number, until we finally have exhausted the remaining digits of the number and the $a - a_m \cdot k^m$ step leaves us with a value of zero.

2 Operations In Base 10 Representation

Now that we can represent numbers in a particular base, how do we add and multiply them in this representation? We don't particularly want to use set theoretic notation as in lesson three. After all, we'd rather write $15 + 17 = 32$ than $15 + 17 = 15' + 16 = 15'' + 15 = \ldots = 15''''''''''''''''' = 16'''''''''''''''' = \ldots = 32$ when adding. The author outright refuses to use set notation to calculate $243 \cdot 128$.

2.1 Preliminary Work: $k^m \cdot k^n$

To complete this section, we must first establish something which may seem obvious: $k^m \cdot k^n = k^{m+n}$. This follows immediately from the definition of an exponent, but should be explicitly shown before continuing: $k^m \cdot k^n = \underbrace{k \cdot k \cdot \ldots \cdot k}_{m \text{ copies}} \cdot \underbrace{k \cdot k \cdot \ldots \cdot k}_{n \text{ copies}} = \underbrace{k \cdot k \cdot \ldots \cdot k}_{m+n \text{ copies}} = k^{m+n}$

2.2 Addition

One would think that addition is very straightforward: if $a = a_m k^m + a_{m-1} k^{m-1} + \ldots + a_2 k^2 + a_1 k^1 + a_0$ and $b = b_n k^n + b_{n-1} k^{n-1} + \ldots + b_2 k^2 + b_1 k^1 + b_0$, then if $a + b = c$ we would expect that (for $m \geq n$)[2] we would have $c = (a_m + b_m) k^m + (a_{m-1} + b_{m-1}) k^{m-1} + \ldots + (a_2 + b_2) k^2 + (a_1 + b_1) k^1 + (a_0 + b_0)$, such that $c_i = a_i + b_i$. This is, after all, both intuitive, and an immediate consequence of the distributive property:

$$
\begin{aligned}
a + b &= a_m k^m + a_{m-1} k^{m-1} + \ldots + a_2 k^2 + a_1 k^1 + a_0 \\
&\quad + b_n k^n + b_{n-1} k^{n-1} + \ldots + b_2 k^2 + b_1 k^1 + b_0 \\
&= a_m k^m + a_{m-1} k^{m-1} + \ldots + a_2 k^2 + a_1 k^1 + a_0 \\
&\quad + b_m k^m + b_{m-1} k^{m-1} + \ldots + b_2 k^2 + b_1 k^1 + b_0 \\
&= (a_m + b_m) k^m + (a_{m-1} + b_{m-1}) k^{m-1} + \ldots \\
&\quad + (a_2 + b_2) k^2 + (a_1 + b_1) k^1 + (a_0 + b_0)
\end{aligned}
$$

where, in the second step, we have added several $b_i = 0$ for each $m \geq i > n$ as needed to force a and b into the same number of digits. There is only one problem left to deal with: there is no guarantee that $(a_i + b_i) < k$ for any given

[2] If $n > m$, then we would sum the terms in the representation of c up to $c_n k^m$ instead of $c_m k^m$ instead. The important things to recognize are that a and b need not have the same number of digits in our representation to a given base, and that they must use the same base k.

i as needed. For this, we will move out of the abstract notation and use the explicit example of $15 + 17$ in base 10.

In our representation, we have $15 = 1 \cdot 10 + 5$ and $17 = 1 \cdot 10 + 7$. Thus, $15+17 = 1 \cdot 10+5+1 \cdot 10+7 = (1+1) \cdot 10+(5+7) = 2 \cdot 10+12$. The $2 \cdot 10$ part is fine, but what do we do with the 12? That is more than one digit, and we're only allowed one digit in each of our numbers. We use the closure property in reverse to remove multiples of 10, and write 12 as $10 + 2$ as follows:

$$15+17 = 2\cdot10+12 = 2\cdot10+10+2 = 2\cdot10+1\cdot10+2 = (2+1)\cdot10+2 = 3\cdot10+2 = 32$$

The classroom terminology for this process has changed from "carrying" to "regrouping" in recent years, to emphasize the idea that you are taking groups of 10 and moving them to another group of digits.

What do we do with larger numbers? For example, what is $796 + 487$? That is as follows:

$$\begin{aligned}
96 + 87 &= 7 \cdot 10^2 + 9 \cdot 10 + 6 + 4 \cdot 10^2 8 \cdot 10 + 7 \\
&= (7 + 4) \cdot 10^2 + (9 + 8) \cdot 10 + (6 + 7) \\
&= (11) \cdot 10^2 + (17) \cdot 10 + (13) \\
&= (10 + 1) \cdot 10^2 + (10 + 7) \cdot 10 + (10 + 3) \\
&= (10 + 1) \cdot 10^2 + (10 + 7 + 1) \cdot 10 + 3 \\
&= (10 + 1 + 1) \cdot 10^2 + 8 \cdot 10 + 3 \\
&= (10 + 2) \cdot 10^2 + 8 \cdot 10 + 3 \\
&= 10^3 + 2 \cdot 10^2 + 8 \cdot 10 + 3 \\
&= 1 \cdot 10^3 + 2 \cdot 10^2 + 8 \cdot 10 + 3 \\
&= 1283
\end{aligned}$$

This clearly works, but the notation gets a little cumbersome. What's the point of writing the numbers compactly, with all the 10^i bits, if we have to write them in the so-called "expanded notation" just to work with them? Well, we don't have to do it that we. Instead, we can use the following compact (and, most likely, familiar) notation:

$$\begin{array}{rr}
 & {\scriptstyle 111} \\
 & 796 \\
+ & 487 \\
\hline
 & 1283
\end{array}$$

Notice that we have aligned our numbers so that the digits with the same place values are written directly above each other. Thus, if we were to add two numbers with differing numbers of digits, they would align on the *right* as follows:

$$\begin{array}{rr} & {\scriptstyle 11} \\ & 796 \\ + & 87 \\ \hline & 883 \end{array}$$

Note also that the extra multiples of 10 we carried through are written smaller, above the digit it will be grouped with, while the portion kept is written below the line at the bottom. For example, the ones digit includes $6+7=13=1\cdot 10+3$, so the 3 was written below the line and the 1 from $1\cdot 10$ was written above the $9+8$ sum, which it will ultimately be grouped into. Then, each digit is found by adding *all* numbers in a column.

2.2.1 Author's Rant: The Sequel

Notice how, in the above example, digits were regrouped starting at the rightmost digit and working up to higher digits. There is a trend towards "constructivism" right now, which is (generally speaking) a good trend: the basic idea is to teach students the way they are naturally inclined to learn, so that the learning process is as smooth and easy as possible, and so that students can build of their present knowledge to move forward. Research has shown this kind of approach leads to faster learning and higher retention. In most cases, it is a very good idea.

One side effect is that there is a trend to teaching students to add, subtract and multiply from left to right instead of right to left, which (in the case of many multiplication problems in particular) ultimately means adding more steps to the computation. This is intuitive for students who speak Latin-based languages which read from left to right. However, the number system used throughout the world was first developed in arabic nations, where the language is read from right to left. Thus, the natural instinct of the student is contrary to the natural order of mathematics when the spoken language is introduced significantly sooner than numbers with more than one digit. This approach is also contained primarily to elementary schools, so when algebra is introduced and *must* function from right to left (as with, say, putting the function f to the left of its argument x in $f(x)$ notation) the student hits the lack of intuition at a new, later time. The problem is not being solved, but merely postponed. This is why the "compute from left to right" approach failed when it was attempted in the mid- to late 19th century in the Latin-based world. The author has yet to see a compelling reason to believe that it will work any better this time (particularly since the curriculum leaders he's spoken to advocating this approach have all been blissfully unaware that it was tried before at all, let alone that it was abandoned as a disaster) and would like to propose and alternative: introduce math to children when introducing language the first time, so that they end up learning to decode words and to add multiple digits numbers at around the same time. Then the opportunity to stress that math and some languages[3] work in opposite ways, because they were invented in different parts of the world. One can even throw in a quick "people from other parts of the world can be just as smart and creative as people from the same place we're from" lesson at the same time, which is entirely unrelated to math, but is an attitude the author would like to see more often. End rant.

2.3 Subtraction

So, if we now know how to add, how do we subtract? Well, subtraction has been defined as adding a negative, such that $a - b = a + (-b)$, where (for brevity) we are assuming that $a > 0$ and $b > 0$. Each digit a_i in our base 10 notation must satisfy $0 \leq a_i < 10$, so clearly negative digits aren't allowed. How do we represent negative numbers? We use the intuitive method of writing a "-" sign in front of the positive number it serves as inverse for, so that the negative of 12345 is -12345. Mathematically, this is equivalent to the expansion

$$\begin{aligned} a &= -(a_m k^m + a_{m-1} k^{m-1} + \ldots + a_2 k^2 + a_1 k^1 + a_0) \\ &= -a_m k^m - a_{m-1} k^{m-1} - \ldots - a_2 k^2 - a_1 k^1 - a_0 \end{aligned}$$

Thus, subtraction initially appears completely intuitive:

$$\begin{aligned} a - b &= a_m k^m + a_{m-1} k^{m-1} + \ldots + a_2 k^2 + a_1 k^1 + a_0 \\ &\quad -b_n k^n - b_{n-1} k^{n-1} - \ldots - b_2 k^2 - b_1 k^1 - b_0 \\ &= a_m k^m + a_{m-1} k^{m-1} + \ldots + a_2 k^2 + a_1 k^1 + a_0 \\ &\quad -b_m k^m - b_{m-1} k^{m-1} - \ldots - b_2 k^2 - b_1 k^1 - b_0 \\ &= (a_m - b_m) k^m + (a_{m-1} - b_{m-1}) k^{m-1} + \ldots \\ &\quad +(a_2 - b_2) k^2 + (a_1 - b_1) k^1 + (a_0 - b_0) \end{aligned}$$

Intuition fails to suffice in cases where $b_i > a_i$, however. For this, we apply the concept of regrouping once more, to draw an additional group of 10 from a

[3] Such as the language this document is written in.

higher digit. Let us use a concrete example with $32 - 17$.

$$\begin{aligned} 32 - 17 &= 3 \cdot 10 + 2 - 1 \cdot 10 - 7 \\ &= (3-1) \cdot 10 + (2-7) \\ &= 2 \cdot 10 + 2 - 7 \\ &= 1 \cdot 10 + 10 + 2 - 7 \\ &= 1 \cdot 10 + 12 - 7 \\ &= 1 \cdot 10 + 5 \\ &= 15 \end{aligned}$$

As with addition, we have developed a more compact notation for this:

$$\begin{array}{rr} & {}^{2\ 12} \\ & \not{3}\not{2} \\ - & 17 \\ \hline & 15 \end{array}$$

Notice that the modified values are written above the original digits, and the original digits are *ignored* in the actual computation. However, there are several other cases that need to be explicitly considered. This works because we *have* the greater number on top. What if we need to compute $a - b$ when $b > a$? Then we will not have access to any powers of 10 from higher digits to regroup. We handle this case by making use of the distributive property and the fact that $(-1) \cdot (-1) = 1$:

$$\begin{aligned} a - b &= a + (-b) = 1 \cdot a + (-1) \cdot b = (-1)^2 \cdot a + (-1) \cdot b = (-1) \cdot ((-1) \cdot (a) + b) \\ &= (-1) \cdot (b - a) \end{aligned}$$

With this formulation, we can compute $b - a$ as above, and then merely take the negative of that answer to finish the problem. Now for the final case with our artificial restriction that $a > 0$ and $b > 0$. What if we have $-a - b$? Again, we use the distributive property:

$$-a - b = (-a) + (-b) = (-1) \cdot a + (-1) \cdot b = (-1) \cdot (a + b)$$

Thus, we simply add a and b, and take the negative of that.

Now, what if our assumption that $a > 0$ and $b > 0$ is false? Well, we could just use new variables $c = -a$ and $d = -b$ and then use the above formulation, which is the most efficient way to handle most cases. We could also note that $-(-a) = a$ for every a, and find that many such cases reduce to cases of addition. In the case where both a and b are negative, for example, we have $a - b = (-c) - (-d) = -c + d = d - c = -(b - a)$. This framework, combined with the distributive property, leads to all of the natural rules and requirements needed to progress effectively.

2.4 Multiplication

Multiplication is the operation for which our preliminary work at the start of this lesson will be most useful. How does one represent and calculate $a \cdot b$ in base 10 representation? One answer is clear when we recognize that multiplication over the integers is interpreted as repeated addition, and thus write $7 \cdot 6 = 7 + 7 + 7 + 7 + 7 + 7$ using our existing framework. While that may work for this case, it's hardy an efficient way to handle something like $243 \cdot 165$. We need something new. We perform this calculation using repeated application of the distributive property, as well as a liberal application of $k^m \cdot k^n = k^{m+n}$, as seen in the following concrete example:

$$
\begin{aligned}
243 \cdot 165 &= \big(2 \cdot 10^2 + 4 \cdot 10 + 3\big) \cdot \big(1 \cdot 10^2 + 6 \cdot 10 + 5\big) \\
&= \big(2 \cdot 10^2 + 4 \cdot 10 + 3\big) \cdot (1 \cdot 10^2) \\
&\quad + \big(2 \cdot 10^2 + 4 \cdot 10 + 3\big) \cdot (6 \cdot 10) \\
&\quad + \big(2 \cdot 10^2 + 4 \cdot 10 + 3\big) \cdot 5 \\
&= \big(2 \cdot 10^2 + 4 \cdot 10 + 3\big) \cdot 10^2 \\
&\quad + \big(12 \cdot 10^2 + 24 \cdot 10 + 18\big) \cdot 10 \\
&\quad + \big(10 \cdot 10^2 + 20 \cdot 10 + 15\big) \\
&= \big(2 \cdot 10^2 + 4 \cdot 10 + 3\big) \cdot 10^2 \\
&\quad + \big(1 \cdot 10^3 + 4 \cdot 10^2 + 5 \cdot 10 + 8\big) \cdot 10 \\
&\quad + \big(1 \cdot 10^3 + 2 \cdot 10^2 + 1 \cdot 10 + 5\big) \\
&= (2+1) \cdot 10^4 + (4+4+1) \cdot 10^3 + (3+5+2) \cdot 10^2 + (8+1) \cdot 10 + 5 \\
&= 3 \cdot 10^4 + 9 \cdot 10^3 + 10 \cdot 10^2 + 9 \cdot 10 + 5 \\
&= 3 \cdot 10^4 + 10 \cdot 10^3 + 0 \cdot 10^2 + 9 \cdot 10 + 5 \\
&= 4 \cdot 10^4 + 0 \cdot 10^3 + 0 \cdot 10^2 + 9 \cdot 10 + 5 \\
&= 40095
\end{aligned}
$$

While this is certainly more efficient than adding 165 copies of 243, or adding 243 copies of 165, it still takes up a lot of space on the page. This is why we tend to take advantage of our addition framework and multiply things out a little more efficiently by working through one digit at a time. We also often use $\times$ instead of $\cdot$ for this representation, to avoid confusion with the decimal places we have not yet established.

$$
\begin{array}{lr}
 & 243 \\
\times & \mathit{1}\mathbf{6}5 \\
\hline
 & 1215 \\
 & \mathbf{14580} \\
 & \mathit{24300} \\
\hline
 & 40095
\end{array}
$$

The bold and italicized typefaces are used to show which digit from the lower number was multiplied into the higher number to produce each row in the sum below. Note also the zeroes on the end; these represent the powers of ten implicit in the place values of the digit involved in the multiplication.

Note also that students are often encourage to place the greater number on top and the lower number on the bottom, for reasons of aesthetics or efficiency. While the aesthetic reasons will vary in their support from individual to individual, the author feels compelled to point out that the most computationally efficient number to put on the bottom row is the one with the fewest *unique, nonzero* digits, particularly if this nonzero digits are 1. For example, if one is multiplying 4444 by 132, one would be trained to compute it as follows:

$$\begin{array}{lr} & 4444 \\ \times & 132 \\ \hline & 8888 \\ & 133320 \\ & 444400 \\ \hline & 586608 \end{array}$$

Each of the three rows being added below the first horizontal line needed to be computed individually. However, as an alternative, one could compute the following:

$$\begin{array}{lr} & 132 \\ \times & 4444 \\ \hline & 528 \\ & 5280 \\ & 52800 \\ & 528000 \\ \hline & 586608 \end{array}$$

Note that, not only have the rows become duplicates (aside from the trailing zeroes) allowing one to use one mental calculation to compute, but that the vertical addition afterwards is also rife with repetition. Granted, there is one more number to add, but the number of *unique* computations to perform is reduced, improving computational efficiency.

2.5 Division

Division will be formally defined in a later lesson. While it is true that, way back in lesson four, we defined division by x as multiplying by the inverse of x, or $x^{-1} = \frac{1}{x}$, we do not yet have a definition for what the inverse of x is for integers. In the not too distant future, we will find a way to define division in a ring which may appear somewhat unfamiliar. When we eventually develop all 11 field axioms, we will be able to formally define division in the sense we are used to for base ten number representation, with decimals.

3 Upcoming Lessons

The lesson will demonstrate the effectiveness of other bases, notably 2, 8 and 16, which are encountered often enough in computer science to be worth studying here. After that, other applications of ring theory will be explored, ultimately leading to the ideas behind some random number generators and encryption algorithms.