

Understanding Decimal Addition

2.1 Experience Versus Understanding

This book is about understanding system architecture in a quick and clean way: no black art, nothing you can only get a feeling for after years of programming experience. While experience is good, it does not replace understanding. For illustration, consider the basic method for decimal addition of one-digit numbers as taught in the first weeks of elementary school: everybody has experience with it, almost nobody understands it; *very* few of the people who do not understand it realize that they don't.

Recall that, in mathematics, there are definitions and statements. Statements that we can prove are called theorems. Some true statements, however, are so basic that there are no even more basic statements that we can derive them from; these are called axioms. A person who understands decimal addition will clearly be able to answer the following simple

Questions: Which of the following equations are definitions? Which ones are theorems? If an equation is a theorem, what is the proof?

$$2 + 1 = 3,$$

$$1 + 2 = 3,$$

$$9 + 1 = 10.$$

We just stated that these questions are simple; we did not say that answering them is easy. Should you care? Indeed you should, for at least three reasons: i) In case you don't even understand the school method for decimal addition, how can you hope to understand computer systems? ii) The reason why the school method works has *very* much to do with the reason why binary addition in the fixed-point adders of processors works. iii) You should learn to distinguish between having experience with something that has not gone wrong (yet) and having an explanation of why it always works. The authors of this text consider iii) the most important.

2.2 The Natural Numbers

In order to answer the above questions, we first consider counting. Since we count by repeatedly adding 1, this should be a step in the right direction.

The set of *natural numbers* \mathbb{N} and the properties of counting are not based on ordinary mathematical definitions. In fact, they are so basic that we use five axioms due to Peano to simultaneously lay down all properties about the natural numbers and of counting we will ever use without proof. The axioms talk about

- a special number 0,
- the set \mathbb{N} of all natural numbers (with zero),
- counting formalized by a *successor* function $S : \mathbb{N} \rightarrow \mathbb{N}$, and
- subsets $A \subset \mathbb{N}$ of the natural numbers.

Peano's axioms are

1. $0 \in \mathbb{N}$. Zero is a natural number. Note that this is a modern view of counting, because zero counts something that could be there but isn't.
2. $x \in \mathbb{N} \rightarrow S(x) \in \mathbb{N}$. You can always count to the next number.
3. $x \neq y \rightarrow S(x) \neq S(y)$. Different numbers have different successors.
4. $\nexists y. 0 = S(y)$. By counting you cannot arrive at 0. Note that this isn't true for computer arithmetic, where you **can arrive** at zero by an overflow of modulo arithmetic (see Sect. 3.2).
5. $A \subseteq \mathbb{N} \wedge 0 \in A \wedge (n \in A \rightarrow S(n) \in A) \rightarrow A = \mathbb{N}$. This is the famous induction scheme for proofs by induction. We give plenty of examples later.

In a proof by induction, one usually considers a set A consisting of all numbers n satisfying a certain property $P(n)$:

$$A = \{n \in \mathbb{N} \mid P(n)\}.$$

Then,

$$\begin{aligned} n \in A &\leftrightarrow P(n), \\ A = \mathbb{N} &\leftrightarrow \forall n \in \mathbb{N} : P(n), \end{aligned}$$

and the induction axiom translates into a proof scheme you might or might not know from high school:

- Start of the induction: show $P(0)$.
- Induction step: show that $P(n)$ implies $P(S(n))$.
- Conclude $\forall n \in \mathbb{N} : P(n)$. Property P holds for all natural numbers.

With the rules of counting laid down by the Peano axioms, we are able to make two 'ordinary' definitions. We define 1 to be the next number after 0 if you count. We also define that addition of 1 is counting.

Definition 1 (Adding 1 by Counting).

$$\begin{aligned} 1 &= S(0), \\ x + 1 &= S(x). \end{aligned}$$

With this, the induction step of proofs by induction can be reformulated to the more familiar form

- Induction step: show that $P(n)$ implies $P(n+1)$.

2.2.1 $2 + 1 = 3$ is a Definition

One can now give meaning to the other digits of decimal numbers with the following mathematical definition.

Definition 2 (The Digits 2 to 9).

$$\begin{aligned} 2 &= 1 + 1 = S(1), \\ 3 &= 2 + 1 = S(2), \\ 4 &= 3 + 1 = S(3), \\ &\vdots \\ 9 &= 8 + 1 = S(8). \end{aligned}$$

Thus, $2 + 1 = 3$ is the definition of 3.

2.2.2 $1 + 2 = 3$ is a Theorem

Expanding definitions, we would like to prove it by

$$\begin{aligned} 1 + 2 &= 1 + (1 + 1) \quad (\text{Definition of 2}) \\ &= (1 + 1) + 1 \\ &= 2 + 1 \quad (\text{Definition of 2}) \\ &= 3 \quad (\text{Definition of 3}). \end{aligned}$$

With the axioms and definitions we have so far we cannot prove the second equation yet. This is due to the fact that we have not defined addition completely. We fix this by the following inductive definition.

Definition 3 (Addition).

$$\begin{aligned} x + 0 &= x, \\ x + S(y) &= S(x + y). \end{aligned}$$

In words: adding 0 does nothing. In order to add $y + 1$, first add y , then add 1 (by counting to the next number). From this we can derive the usual laws of addition.

Lemma 1 (Associativity of Addition).

$$(x + y) + z = x + (y + z).$$

Proof. by induction on z . For $z = 0$ we have

$$(x + y) + 0 = x + y = x + (y + 0)$$

by definition of addition (adding 0).

For the induction step we assume the induction hypothesis $x + (y + z) = (x + y) + z$. By repeatedly applying the definition of addition we conclude

$$\begin{aligned} (x + y) + S(z) &= S((x + y) + z) \quad (\text{by definition of addition}) \\ &= S(x + (y + z)) \quad (\text{by induction hypothesis}) \\ &= x + S(y + z) \quad (\text{by definition of addition}) \\ &= x + (y + S(z)). \end{aligned}$$

Substituting $x = y = z = 1$ in Lemma 1, we get

$$(1 + 1) + 1 = 1 + (1 + 1)$$

which completes the missing step in the proof of $1 + 2 = 3$.

Showing the commutativity of addition is surprisingly tricky. We first have to show two special cases.

Lemma 2. $0 + x = x$.

Proof. by induction on x . For $x = 0$ we have

$$0 + 0 = 0$$

by the definition of addition.

For the induction step we can assume the induction hypothesis $0 + x = x$ and use this to show

$$\begin{aligned} 0 + S(x) &= S(0 + x) \quad (\text{definition of addition}) \\ &= S(x) \quad (\text{induction hypothesis}). \end{aligned}$$

Lemma 3. $x + 1 = 1 + x$.

Proof. by induction on x . For $x = 0$ we have

$$0 + 1 = 1 = 1 + 0$$

by the previous lemma and the definition of addition.

For the induction step we can assume the induction hypothesis $x + 1 = 1 + x$ and show

$$\begin{aligned} 1 + S(x) &= S(1 + x) \quad (\text{definition of addition}) \\ &= S(x + 1) \quad (\text{induction hypothesis}) \\ &= S(x) + 1 \quad (\text{definition of counting by adding 1}). \end{aligned}$$

Lemma 4 (Commutativity of Addition).

$$x + y = y + x.$$

Proof. by induction on y . For $y = 0$ we have

$$\begin{aligned} x + 0 &= x \quad (\text{definition of addition}) \\ &= 0 + x \quad (\text{Lemma 2}). \end{aligned}$$

For the induction step we can assume the induction hypothesis $x + y = y + x$ and show

$$\begin{aligned} x + S(y) &= S(x + y) \quad (\text{definition of addition}) \\ &= S(y + x) \quad (\text{induction hypothesis}) \\ &= y + S(x) \quad (\text{definition of addition}) \\ &= y + (x + 1) \quad (\text{definition of counting by adding 1}) \\ &= y + (1 + x) \quad (\text{Lemma 3}) \\ &= (y + 1) + x \quad (\text{associativity of addition}) \\ &= S(y) + x \quad (\text{definition of counting by adding 1}). \end{aligned}$$

By induction one shows the following in the same way.

Lemma 5.

$$\begin{aligned} (x + y) \cdot z &= x \cdot z + y \cdot z \quad (\text{distributivity}), \\ (x \cdot y) \cdot z &= x \cdot (y \cdot z) \quad (\text{associativity of multiplication}), \\ x \cdot y &= y \cdot x \quad (\text{commutativity of multiplication}). \end{aligned}$$

The proof is left as an exercise.

2.2.3 $9 + 1 = 10$ is a Brilliant Theorem

The proof of $9 + 1 = 10$ is much more involved. It uses a special biological constant defined as

$$Z = 9 + 1$$

which denotes the number of our fingers or, respectively, toes¹. Moreover it uses a definition attributed to the brilliant mathematician al-Khwarizmi, which defines the decimal number system.

Definition 4 (Decimal Numbers). An n -digit decimal number $a_{n-1} \dots a_0$ with digits $a_i \in \{0, \dots, 9\}$ is interpreted as

$$a_{n-1} \dots a_0 = \sum_{i=0}^{n-1} a_i \cdot Z^i.$$

¹ We use the letter Z here because in German, our native language, the word for ‘ten’ is ‘zehn’ and the word for ‘toes’ is ‘Zehen’, thus it’s almost the same.

Substituting $n = 2$, $a_1 = 1$, and $a_0 = 0$ we can derive the proof of $9 + 1 = 10$. We must however evaluate the formula obtained from the definition of decimal numbers; in doing so, we need properties of exponentiation and multiplication:

$$\begin{aligned}
 10 &= 1 \cdot Z^1 + 0 \cdot Z^0 && \text{(definition of decimal number)} \\
 &= 1 \cdot Z + 0 \cdot 1 && \text{(properties of exponentiation)} \\
 &= Z + 0 && \text{(properties of multiplication)} \\
 &= Z && \text{(definition of addition)} \\
 &= 9 + 1 && \text{(definition of } Z\text{).}
 \end{aligned}$$

Observe that addition and multiplication are taught in elementary school, whereas exponentiation is only treated much later in high school. In this order we cannot possibly fill the gaps in the proof above. Instead, one defines multiplication and exponentiation without relying on decimal numbers, as below.

Definition 5 (Multiplication).

$$\begin{aligned}
 x \cdot 0 &= 0, \\
 x \cdot S(y) &= x \cdot y + x.
 \end{aligned}$$

Definition 6 (Exponentiation).

$$\begin{aligned}
 x^0 &= 1, \\
 x^{S(y)} &= x^y \cdot x.
 \end{aligned}$$

By Lemma 2 we get

$$x \cdot 1 = x \cdot (S(0)) = x \cdot 0 + x = 0 + x = x.$$

i.e., multiplication of x by 1 from the right results in x . In order to progress in the proof of $9 + 1 = 10$, we show the following.

Lemma 6. $1 \cdot x = x$.

Proof. by induction on x . For $x = 0$ we have

$$1 \cdot 0 = 0$$

by the definition of multiplication.

For the induction step we can assume the induction hypothesis $1 \cdot x = x$ and show

$$\begin{aligned}
 1 \cdot S(x) &= 1 \cdot x + 1 && \text{(definition of multiplication)} \\
 &= x + 1 && \text{(induction hypothesis).}
 \end{aligned}$$

Using Lemma 6, we get

$$x^1 = x^{S(0)} = x^0 \cdot x = 1 \cdot x = x. \tag{1}$$

We finish the section by showing a classical identity for exponentiation.

Lemma 7. $x^{y+z} = x^y \cdot x^z$.

Proof. by induction on z . For $z = 0$ we have (leaving the justification of the steps as an exercise)

$$x^{y+0} = x^y = x^y \cdot 1 = x^y \cdot x^0.$$

For the induction step we assume the induction hypothesis $x^{y+z} = x^y \cdot x^z$ and show

$$\begin{aligned} x^{y+S(z)} &= x^{S(y+z)} && \text{(definition of addition)} \\ &= x^{(y+z)} \cdot x && \text{(definition of exponentiation)} \\ &= (x^y \cdot x^z) \cdot x && \text{(induction hypothesis)} \\ &= x^y \cdot (x^z \cdot x) && \text{(associativity of multiplication, Lemma 5)} \\ &= x^y \cdot (x^{S(z)}) && \text{(definition of exponentiation).} \end{aligned}$$

2.3 Final Remarks

Using decimal addition as an example, we have tried to convince the reader that being used to something that has not gone wrong yet and understanding it are very different things. We have reviewed Peano's axioms and have warned the reader that computer arithmetic does not satisfy them. We have formally defined the value of decimal numbers; this will turn out to be helpful, when we study binary arithmetic and construct adders later. We have practiced proofs by induction and we have shown how to derive laws of computation without referring to decimal representations.

We recommend to remember as key technical points:

- Peano's axioms.
- the inductive definition of addition as iterated counting

$$\begin{aligned} x + 0 &= x, \\ x + (y + 1) &= (x + y) + 1. \end{aligned}$$

- for parties: $2 + 1 = 3$, $1 + 2 = 3$, $9 + 1 = 10$. Which are theorems?

Everything else is easy. Rules of computation are shown by induction; what else can you do with an inductive definition of addition? And of course multiplication is defined by iterated addition and exponentiation is defined by iterated multiplication.

A proof of the usual rules of computation governing addition, subtraction, multiplication, and division of the rational numbers and/or the real numbers can be found in [Lan30]. The recursive definitions of addition, multiplication, and exponentiation that we have presented also play a central role in the theory of computability [Rog67, Pau78].

2.4 Exercises

1. For each of the following statements, point out which ones are definitions and which ones are theorems for $x, y \in \mathbb{N}$. Prove the theorems using only definitions and statements proven above.
 - a) $x = x + 0$,
 - b) $x = 0 + x$,
 - c) $x + (y + 1) = (x + y) + 1$,
 - d) $(x + 1) + y = (y + x) + 1$,
 - e) $x \cdot 0 = 0$,
 - f) $0 \cdot x = 0$,
 - g) $5 + 1 = 6$,
 - h) $7 + 4 = 11$.
2. Prove Lemma 5.
3. Prove the following properties of exponentiation for $a, b, c \in \mathbb{N}$.

$$(a \cdot b)^c = a^c \cdot b^c,$$

$$(a^b)^c = a^{b \cdot c}.$$

4. We define a modified subtraction of natural numbers

$$-': \mathbb{N} \rightarrow \mathbb{N}$$

by

$$x -' y = \begin{cases} x - y, & x \geq y, \\ 0, & \text{otherwise.} \end{cases}$$

Give an inductive definition of this function, starting with the successor function $S(x)$.

Hint: clearly you want to define a modified decrement function $D(x) = x -' 1$ first. Do this by an inductive definition.

System Architecture

An Ordinary Engineering Discipline

Paul, W.J.; Baumann, C.; Lutsyk, P.; Schmaltz, S.

2016, XII, 512 p. 243 illus., Hardcover

ISBN: 978-3-319-43064-5