1. Basic Notions

04/11/2019.

Real analysis is the study of real numbers, sequences and series of real numbers and real-valued functions. This is related to, but distinct from complex analysis, which concerns the analysis of complex numbers and complex functions, harmonic analysis, which concerns the analysis of harmonics (waves) such as sine waves, and how they synthesize other functions via the Fourier transform, functional analysis, which focuses much more heavily on functions (and how they form things like vector spaces) and so forth. Analysis is the rigorous study of such objects, with a focus on trying to pin down precisely and accurately, the qualitative and quantitative behaviour of these objects. Real analysis is the theoretical foundation which underlies calculus, which is the collection of computational algorithms which one uses to manipulate functions.

In this course, we will be studying many objects which are familiar from freshman calculus: numbers, sequences, series, limits, functions, definite integrals, derivatives and so forth. We already have a great deal of experience computing with these objects, however, here we will be more focused on the underlying theory ~~with~~ for these objects. We will be concerned with questions such as the following —

1. What is a real number? Is there a largest real number? After 0, what is the next real number? (that is what is the smallest positive real number?) Can you cut a real number into pieces infinitely many times? Why does a number such as 2 have a square root, while a number such as −2 does not? If there are infinitely many reals and infinitely many rationals, how come there are "more" real numbers than rational numbers?

2. How do you take the limit of a sequence of real numbers? Which sequences have limits and which ones don't? If you can stop a sequence from escaping to ~~unity~~ infinity, does this mean, it will eventually settle and converge? Can you add infinitely many real numbers together and still get a finite number? Can you add infinitely many rational numbers together and end up with a non-rational number? If you rearrange the elements of an infinite sum, is the sum still the same?

3. What is a function? What does it mean for a function to be continuous? differentiable? integrable? bounded? Can you add infinitely many functions together? What about taking limits of sequences of functions? Can you differentiate and infinite series of functions? What about integrating? If a function $f(x)$ takes the value 3 when $x=0$ and 5 when $x=1$ (that $f(0)=3$, $f(1)=5$), does it have to take every intermediate value between 3 and 5, when x goes between 0 and 1.

In this course, we will review the material learnt in high school and in elementary calculus classes, but as rigorously as possible. To do so, we will have to begin at the very basics - indeed we will go back to the concept of ~~nat~~ numbers and what their properties are. Of course, we have dealt with numbers for over ten years and know how to manipulate the rules of algebra to simplify any expression involving numbers, but we will now turn to a more fundamental issue, which is: why do the rules of algebra work at all? For instance, why is it true that $a(b+c) = ab + ac$ for any three numbers a, b, c.

In the first few chapters, we reacquaint our-selves with various number systems that are used in real analysis. In increasing order of sophistication, they are the natural numbers $\mathbb{N}$, the integers $\mathbb{Z}$, the rationals $\mathbb{Q}$ and the real numbers $\mathbb{R}$.

1. Natural Numbers.

We will consider the following question: how does one actually define the natural numbers. (This is very different question from how to use the natural numbers, which is something you of course know how to do well. It's like the difference between knowing how to use, say, a computer, versus knowing how to build that computer.)

This question is more difficult to answer than it looks. The basic problem is that we have used the natural numbers for so long that they are deeply embedded into our mathematical thinking and we can make various implicit assumptions about these numbers (e.g. that $a+b=b+a$) without even aware that we are doing so; it is difficult to let go and try to inspect this number system as if it is the first time we have seen it. So, in what follows I will have to ask you to perform a rather difficult task: try to set aside, for the moment, everything you know about the natural numbers; forget that you know how to count, to add, to multiply, to manipulate the rules of algebra etc. We introduce these concepts one at a time and identify explicitly what our assumptions are as we go along – and not allow ourselves to use more "advanced" tricks such as the rules of algebra until we have actually proven them. This may seem like an irritating constraint, especially as we will spend alot of time proving statements which are obvious, but it is necessary to do this suspension of known facts to avoid circularity (e.g. using an advanced fact to prove a more elementary fact, and then later using the elementary fact to prove the advanced fact). Also, this exercise will be an excellent way to affirm the foundations of your mathematical knowledge. Furthermore, practicing your proofs and abstract thinking here will be invaluable when we move on to more advanced concepts, such as real numbers, functions, sequences and series, differentials and integrals and so forth. In short, the results here may seem trivial, but the journey is much more important than the destination for now. (Once the number systems are constructed properly, we can resume using the laws of algebra etc. without having to rederive them each time.)

We will also forget that we know the decimal ~~number~~ system, which is of course an extremely convenient way to manipulate numbers, but it is not something which is fundamental to what numbers are. (For instance, we could use an octal or binary system instead of the decimal system, or even the roman numeral system and still get exactly the same set of numbers.) Besides if one tries to fully explain what the decimal number system is, it isn't as natural as you might think. Why is 00423 the same number as 423, but 32400 isn't the same number as 324? Why is 123.444... a real number, while ...444.321 is not? And why do we have to carry off digits when adding or multiplying? Why is 0.999... the same number as 1? What is the smallest positive real number? Isn't it just 0.00...01? So, to set aside these problems, we will not try to assume any knowledge of the decimal system, though we will of course refer to numbers by their familiar names such as 1, 2, 3 etc. instead of using other notation such as I, II, III or 0++, (0++)++, ((0++)++)++, so as not to be needlessly artificial.

We now present one standard way to define natural numbers in terms of the Peano axioms, which were first laid out by Guiseppe Peano (1858–1932). This is not the only way to define the natural numbers. For instance, another approach is to talk about the cardinality of finite sets, for instance one could take a set of five elements and define 5 to be the number of elements in that set. We shall discuss this alternate approach at length later. We shall stick to the Peano axiomatic approach for now.

Definition ~~(Informal)~~. A natural number is any element of the set

$$\mathbb{N} := \{0, 1, 2, 3, 4, 5, \ldots\}.$$

which is the set of all the numbers created by starting with 0 and then counting forward indefinitely. We call $\mathbb{N}$ the set of natural numbers.

In a sense, this definition solves the ~~question~~ problem of what the natural numbers are: a natural number is any element of the set $\mathbb{N}$. However, it is not really that satisfactory, because it begs the definition of what $\mathbb{N}$ is. This definition of start at 0 and count indefinitely seems like an intuitive enough definition of $\mathbb{N}$, but it is not entirely acceptable, because it leaves many questions unanswered. For instance: how do we know we can keep counting indefinitely without cycling back to 0? Also how do we perform operations such as addition, multiplication, or exponentiation?

We can answer the latter question first: we can define complicated operations in terms of simpler operations. Exponentiation is nothing more than repeated multiplication: 5^3 is nothing but $5 \times 5 \times 5$. Multiplication is nothing more than repeated addition: 5×3 is nothing more than $5+5+5$. (Subtraction and division will not be covered here; they will have to wait for the integers and rationals, respectively. And addition? It is nothing more than the repeated operation of counting forward, or incrementing. If you add 3 to 5, what you are doing is incrementing 5 three times. On the other hand, incrementing seems to be a more fundamental operation, not reducible to any simpler operation; indeed it is the first operation one learns on numbers, even before learning to add.

Thus, to define the natural numbers, we will use two fundamental concepts: the zero number 0 and the increment operation. In deference to modern computer languages, we will use $n{+}{+}$ to denote the increment or the successor of n, thus for instance $3{+}{+} = 4$, $(3{+}{+}){+}{+} = 5$ etc. This is a slightly different usage from that in computer languages such as C, where $n{+}{+}$ actu redefines the value of n to be its successor; however in mathematics we try not to define a variable more than once in any given setting, as it can often lead to confusion.

So, it seems like we want to say that $\mathbb{N}$ consists of 0 and everything which can be obtained from 0 by counting forward: $\mathbb{N}$ should consist of the objects -

$$0,\ 0{+}{+},\ (0{+}{+}){+}{+},\ ((0{+}{+}){+}{+}){+}{+},\ \text{etc.}$$

If we start writing down what this means about natural numbers we thus see that we should have the following axioms concerning 0 and the increment operation ++.

Axiom 1. 0 is a natural number.
Axiom 2. If n is a natural number, then the successor of n, $n{+}{+}$ is also a natural number.

Thus, for instance, from axiom 1 and two applications of axiom 2, we see that $(0{+}{+}){+}{+}$ is a natural number. Of course, this notation begins to get unwieldy, so we adopt a convention to write these numbers in more familiar notation.

Definition. We define 1 to be the number $0{+}{+}$, 2 to be the number $(0{+}{+}){+}{+}$, 3 to be the number $((0{+}{+}){+}{+}){+}{+}$, etc. (In other words, $1 := 0{+}{+}$, $2 := 1{+}{+}$, $3 := 2{+}{+}$ etc. In this text, I use "$x := y$"

Proposition. 3 is a natural number.

Proof. By axiom 1, 0 is a natural number. By axiom 2, the successor of any natural number n, is also a natural number. So, $0{+}{+} = 1$ is a natural number. Again $1{+}{+} = 2$ is a natural number. Finally, $2{+}{+} = 3$ is a natural number.

It may seem that this is enough to describe the natural numbers. However, we have not completely pinned down the behavior of $\mathbb{N}$.

Examples.
1) Consider a number system which consists of the numbers 0, 1, 2, 3 in which the increment operation wraps back from 3 to 0. More precisely $0{+}{+}$ is equal to 1, $1{+}{+}$ is equal to 2, $2{+}{+}$ is equal to 3, but $3{+}{+}$ is equal to 0 (and also equal to 4, by the definition of 4). This type of thing actually happens in real life, when one uses a computer to try to store a natural number: if one starts at 0 and performs the increment operation repeatedly, eventually the computer will overflow its memory and the number will wrap around back to 0 (though this may take quite a large number of incrementation operations, for instance a 2-byte representation of an integer will wrap around only after 65,536 increments.) Note that this type of number system obeys axiom 1 and axiom 2 event though it clearly does not correspond to what we believe intuitively believe the natural numbers to be like.

To prevent this sort of wrap-around issue we will impose another axiom:

Axiom 3. 0 is not the successor of any natural number. That is, we have $n{+}{+} \neq 0$ for every natural number n.

Now we can show that ~~so~~ certain types of wrap-around do not occur: for instance, we can now rule out the type of behavior in the example using the below proposition

Proposition. 4 is not equal to 0.

Don't laugh! Because of the way we have defined 4 — it is the increment of the increment of the increment of the increment of 0. — it is not necessarily true a priori, that this number is not the same as zero, even if it is obvious. Note for instance, in the example discussed before, 4 was indeed equal to 0 and that in a standard two byte computer representation of a natural number, for instance, 65536 is equal to 0 (using our definition of 65536 as equal to 0 incremented 65536 times)

Proof. By definition $4 = 3{+}{+}$. By axioms 1 and 2, 3 is a natural number. Thus, by axiom 3, $3{+}{+} \neq 0 \Rightarrow 4 \neq 0$.

However, even with our new axiom, it is still possible that our number system behaves in pathological ways.

Examples

1) Consider a number system consisting of five numbers 0, 1, 2, 3, 4, in which the increment operation hits a ceiling at 4. More precisely, suppose that $0{+}{+} = 1$, $1{+}{+} = 2$, $2{+}{+} = 3$, $3{+}{+} = 4$, but $4{+}{+} = 4$ (or in other words that $5 = 4$, and hence $6 = 4$, $7 = 4$ etcetera). This does not contradict the axioms 1, 2 and 3. Another number system with a similar problem is one in which the incrementation wraps around but not to 0 e.g. suppose that $4{+}{+} = 1$ (so that $5 = 1$, then $6 = 2$, etcetera)

There are many ways to prohibit the above types of behavior from happening, but one of the simplest is to assume the following axiom:

Axiom 4. Different natural numbers must have different successors. That is, if n, m are natural numbers and $n \neq m$, then $n{+}{+} \neq m{+}{+}$. Equivalently, if $n{+}{+} = m{+}{+}$, then we must have $n = m$.

Proposition. 6 is not equal to 2.

Proof. Suppose for the sake of contradiction that $6 = 2$. Then, $5{+}{+} = 1{+}{+}$. So by axiom 4, we have $5 = 1$, so that $4{+}{+} = 0{+}{+}$. By axiom 4 again, we then have $4 = 0$, which contradicts our previous proposition.

As one can see from this proposition, it now looks like we can keep all of the natural numbers distinct from each other. There is however still one more problem: while axioms 1 and 2 allows us to confirm that 0, 1, 2, 3, ... are distinct elements of ~~N~~ $\mathbb{N}$, there is the problem that there may be other rogue elements in our number system which are not of this form:

2) Suppose that our number system $\mathbb{N}$ consisted of the following collection of integers and half-integers:

$$\mathbb{N} := \{0, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, \ldots\}.$$

(This example is informal, since we are using real numbers which we are not supposed to use yet.) One can check that axioms 1–4 are still satisfied for this set.

What we want is some axiom which says that the only numbers in $\mathbb{N}$ are those which can be obtained from 0 and the increment operation — in order to exclude elements such as 0.5. But, it is difficult to quantify what we mean by "can be obtained from", without already having the natural numbers, which we are trying to define. Fortunately, there is an ingenious solution to try to capture this fact —

Axiom 5. (Principle of mathematical Induction).
Let $P(n)$ be any statement about the natural number n. Suppose that $P(0)$ is true and suppose that whenever $P(n)$ is true, $P(n{+}{+})$ is also true. Then, $P(n)$ is true for every natural number n.

Remark. We are a little vague on what property means at this point, but some possible examples of $P(n)$ might be "n is even"; "n is equal to 3"; "n solves the equation $(n+1)^2 = n^2+2n+1$ and so forth. Of course, we haven't defined many of these concepts yet, but when we do axiom 5 will apply to these properties. (A logical remark — Because this axiom refers not just to variables, but also properties, it is of a different nature than the other four axioms; indeed axiom 5 should technically be called an axiom schema rather than an axiom — it is a template for producing an infinite number of axioms, rather than being a single axiom in its own right. To discuss this distinction further is far beyond the scope of this course, though, and falls in the realm of logic.

The informal intuition behind this axiom is the following. Suppose $P(n)$ is such that $P(0)$ is true, and such that whenever $P(n)$ is true $P(n{+}{+})$ is true. Then since $P(0)$ is true, $P(0{+}{+}) = P(1)$ is true. Since $P(1)$ is true, $P(1{+}{+}) = P(2)$ is true. Repeating this indefinitely, we see that $P(0), P(1), P(2), P(3)$ etc are all true. However this line of reasoning will never let us conclude that $P(0.5)$ for instance is true. Thus, axiom 5 should not hold for number systems which contain unnecessary elements such as 0.5. (Indeed one can give a proof of this fact. Apply axiom 5 to the property $P(n) = n$ "is not a half integer", ie an integer plus 0.5. Then, $P(0)$ is true and if $P(n)$ is true, $P(n{+}{+})$ is true. Thus, axiom 5 asserts that $P(n)$ is true for all natural numbers n, that is no natural number can be a half integer. In particular, 0.5 cannot be a natural number. This proof is not quite genuine, because we have not quite defined such notions as "integer", "half-integer" and 0.5 yet, but it should give you some ideas as to how the principle of induction is supposed to prohibit any numbers other than the "true" natural numbers from appearing in $\mathbb{N}$.

The principle of induction gives us a way to prove that a property $P(n)$ is true for every natural number n. Thus, in the rest of this text we will see many proofs which have a form like this:

Proposition. A certain property $P(n)$ is true for every natural number n.

Proof.
We use induction. We first verify the base case $n=0$ i.e. prove $P(0)$. (Insert the proof of $P(0)$ here). Now suppose inductively that n is a natural number and $P(n)$ has already been

been proven. We now prove P(n+1). (Insert proof of P(n+1), assuming that P(n) is true, here.) This closes the induction, and thus P(n) is true for all numbers n.

Q.E.D

Of course, we will not necessarily use the exact template, wording or order in the above type of proof, but the proofs using induction will generally be something like the above form. There are also some other variants of induction which we shall encounter later, such as backwards induction, strong induction and transfinite induction.

Axioms 1-5 are called the Peano axioms for the natural numbers. They are all very plausible and so we shall make -

Assumption. There exists a number system $\mathbb{N}$, whose elements we will call natural numbers, for which axioms 1 to 5 are true. We will

We will make this assumption a bit more precise once we have laid down our notation for sets and functions in the next chapter.

A remarkable accomplishment of modern analysis is that just by starting from these five primitive axioms, and some additional axioms from set theory, we can build all the other number systems, create functions and do all the algebra and calculus that we are used to.

Here is another way to view axiom 5.

A subset of $\mathbb{N}$ which contains 0, and which contains $n+1$, whenever it contains n, must equal $\mathbb{N}$.

Proof

- Assume that $\mathbb{N} \not\subseteq S_2$ contains a set S such that,
  1) $0 \in S$
  2) If $n \in S$, $n+1 \in S$.

and yet $S \neq \mathbb{N}$. Consider the set $\{x \in \mathbb{N} : x \notin S\}$. Let n_0 be the smallest member of this set. Since (1) holds, $n_0 \neq 1$. Therefore, n_0 is a successor to some element $n_0 - 1$ in $\mathbb{N}$. We have $n_0 - 1 \in S$, since n_0 is the smallest member of $\{x \in \mathbb{N} : x \notin S\}$. By (ii) if $n_0 - 1 \in S$, the successor of $n_0 - 1$, namely n_0 belongs to S, which is a contradiction.

Thus, $S = \mathbb{N}$.

Remark -

One interesting feature about the natural numbers is that while each individual natural number is finite, the set of natural numbers is infinite, that is $\mathbb{N}$ is infinite, but consists individually of finite elements. (The whole is greater than any of its parts). There are no infinite natural numbers; one can even prove this axiom 5, provided one is comfortable with the notions of finite and infinite. Clearly 0 is finite. Also, if n is finite, $n+1$ is finite. Hence, by axiom 5 all natural numbers are finite. So, the natural number can approach infinity, but never actually reach it, but infinity is not one of the natural numbers.

Remark. Note that our definition of natural numbers is axiomatic rather than constructive. We have not told you what the natural numbers are (so we do not address such questions as what the numbers are made up of, are they of physical objects, what do they measure, etc.) - we have only listed some things you can do with them. (in fact, the only operation we have defined on them right now is the increment one) - and some of the properties that they have. This is how mathematics works - it treats objects abstractly, caring only about what properties the objects have, not what the objects are what they mean. If one wants to do mathematics, it does not matter whether a natural number means a certain arrangement of beads on an abacus, or a certain organization of bits in a computer's memory, or some more abstract concept with no physical significance; as long as you can increment them, see if two of them are equal, and later on do arithmetic operations such as add and multiply, they qualify as numbers for mathematical purposes (provided they obey the requisite axioms of course). It is possible to construct the natural numbers from other mathematical objects - from sets for instance - but there are multiple ways to construct a working model of the natural numbers and it is pointless, atleast from a mathematician's standpoint, as to argue about which model is the true. - as long as it obeys all the axioms and does all the right things, thats good enough to do maths.

Remark. Historically, the realization that numbers could be treated axiomatically is very recent, not much more than a hundred years old. Before then, the numbers were generally understood to be ~~intricately~~ inextricably connected to some external concept, such as counting the cardinality of the set, measuring the length of a line segment, or the mass of a physical object. etc. This worked reasonably well, until one was forced to move from one number system to another; for instance understanding numbers in terms of beads is great counting beads is great, for instance, for conceptualizing the numbers such as 3 and 5, but doesn't work so well for -3 or $1/3$ or $\sqrt{2}$ or $3+4i$; thus each great advance in the theory of numbers - negative numbers, irrational numbers, complex numbers, even the number zero - led to a lot of unnecessary philosophical anguish.

The great discovery of the late nineteenth century was that numbers can be understood abstractly via axioms, without necessarily needing a concrete model; of course a mathematician can use any of these models when it is convenient, to aid his or her intuition and understanding, but they can just as easily be discarded when they begin to get in the way.

One consequence of the axioms is that we can now define sequences recursively. Suppose we want to build a sequence $a_0, a_1, a_2, \ldots$ of numbers by first defining a_0 to be some base value, e.g. $a_0 := c$ for some number c, and then letting a_1 be some function of a_0, $a_1 := f_0(a_0)$, a_2 be some function of a_1, $a_2 := f_1(a_1)$, and so forth. In general, we set $a_{n++} := f_n(a_n)$ for some function f_n from $\mathbb{N}$ to $\mathbb{N}$. By using all axioms together, we will now conclude that this procedure will give a single value to the sequence element a_n for each natural number n.

More precisely: 12/11/2014.

Proposition. Suppose for each natural number n, we have some function $f_n : \mathbb{N} \to \mathbb{N}$ from the natural numbers to the natural numbers. Let c be a natural number. Then we can assign a unique natural number a_n to each natural number n, such that $a_0 = c$ and $a_{n++} = f_n(a_n)$ for each natural number n.

Proof. (Informal). We use mathematical induction. We are required to prove that there is unique function f_n that satisfies the two clauses

$$a_0 = f(0) = c$$
$$a_{n++} = f_n(a_n).$$

Clearly, a single value $f(0) = c$ is assigned to a_0. We assume that a single value is assigned to a_n, so $f_n(a_n)$ is unique since f_n is function. Hence, a single value is assigned to a_{n++}. As a result, all that is needed is a value of $f(0)$ and a way to compute a_{n++} in terms of n and $f(n)$. These two conditions specify all values of the function f, and therefore f is unique.

Note how all of the axioms had to be used here. In a system, which had some sort of a wrap around issue, recursive definitions would not work, because some elements of the sequence would constantly be redefined. For instance, in ~~to~~ the example where the number system wraps back around to zero after counting forward ~~for~~ from 3, $3++ = 0$, then there would be atleast two conflicting definitions of a_0, either c or $f_3(a_3)$. In a systems which had superfluous elements, the number $a_{0.5}$ would never be defined.

Recursive definitions are very powerful, for instance, we can use them to define addition and multiplication, to which we now turn.

Addition of Natural numbers.

The natural number system is very bare right now: we have only one operation - increment - and a handful of axioms. But now we can build up more complex operations such as addition.

The way it works is the following. To add three to five should be the same as incrementing five three times. - this is one increments more than adding two to five, which is one increment more than adding one to five, which is one increment more than adding zero to 5, which should just give five. So we give a recursive definition of addition as follows.

Definition (Addition of natural numbers)

Let m be a natural number. To add zero to m, we define $0 + m := m$. Now suppose inductively we have defined how to add n to m. Then, we can add $n{++}$ to m by defining $(n{++}) + m := (n + m){++}$.

Thus, $0 + m$ is m, $1 + m = (0{++}) + m = (m){++}$; ~~2 +~~

$2 + m = (1{++}) + m = (1 + m){++} = (m{++}){++}$.

$3 + m = (2{++}) + m = (2 + m){++} = ((1{++}) + m){++} = ((1 + m){++}){++} = ((m{++}){++}){++}$

and so forth.

For instance, we have

$$\begin{aligned} 2+3 &= (3++)++ \\ &= 4++ \\ &= 5. \end{aligned}$$

From our discussion of recursion in the previous section we see that we have defined $n+m$ for every natural number n. Here, we are specializing the previous discussion where

$$a_0 = m = f(0)$$
$$a_{n++} = f(a_n) = a_n++$$

Then,

$$\begin{aligned} a_0 &= m \\ a_1 &= a_0++ = m++ \\ a_2 &= a_1++ = (m++)++ \\ a_3 &= a_2++ = ((m++)++)++ \\ &\vdots \\ a_n &= a_{n-1}++ = \underbrace{((m++)++)++\ldots}_{n \text{ times}} \end{aligned}$$

The principle of recursive definition is a fundamental property of the natural numbers.

Note that the above definition of addition is asymmetric: $3+5$ is incrementing 5 three times, while $5+3$ is incrementing 3 five times. Of course, they both yield the same value of 8. More generally, it is a fact (which we shall prove shortly) that $a+b=b+a$ for all natural numbers a, b although this is not immediately clear from the definition. Notice that we can prove easily using axioms 1, 2 and induction that the sum of two natural numbers is again a natural number.

Proof.

Let $P(n)$ be the property that sum of two natural numbers n, m (~~fixed~~) is also a natural number. We keep m fixed, induct on n.

$P(0)$ holds. $0+m := m$. And, m is natural.

Assume that $P(n)$ holds.
Let us assume $(n+m)$ is a natural number.

Claim. $P(n++)$ is true.

$P(n++)$: $(n++)+m := (n+m)++$ Definition of addition.

But, from our assumption above $(n+m)$ is a natural number. From Peano's axioms, if p is a natural number, its successor $p++$ is also a natural number. Hence, $(n+m)++$ is also a natural number. $P(n)$ is true for all $n \in \mathbb{N}$.

Q.E.D.

Right now, we have only two facts about addition: that $0+m=m$, and that $(n++)+m := (n+m)++$. Remarkably, this turns out to be enough to deduce everything else we know about addition.

We begin with some basic lemmas.

13/11/2014

Lemma. For any natural number n, $n+0=n$.
Note that we cannot deduce this immediately from $0+m=m$ because we do not yet know that $a+b=b+a$.

Proof. We use induction. The base case $0+0=0$ follows since we know that $0+m=m$ for every natural number m, and 0 is a natural number. Now, suppose inductively $n+0=n$. We wish to show that $(n{+}{+})+0=n{+}{+}$. But by definition of addition, $(n{+}{+})+0=(n+0){+}{+}=n{+}{+}$, since $n+0=n$. This closes the induction.

Lemma. For any natural numbers n and m, $n+(m{+}{+})=(n+m){+}{+}$.
Again, we cannot deduce this yet from $(n{+}{+})+m=(n+m){+}{+}$ because we do not know yet that $a+b=b+a$.

Proof
We induct on n (keeping m fixed). ~~$n=0$~~ We first consider the base case $n=0$. In this case, ~~$0+(m{+}{+})$~~ we have to prove that $0+(m{+}{+})=(0+m){+}{+}$. But, by definition of addition $0+(m{+}{+})=m{+}{+}$ and $0+m=m$, so both sides are equal to $m{+}{+}$ and are thus equal to each other. We assume inductively that $n+(m{+}{+})=(n+m){+}{+}$. We now have to show that $(n{+}{+})+(m{+}{+})=((n{+}{+})+m){+}{+}$. Indeed, ~~we~~ the left-hand side is — $(n{+}{+})+(m{+}{+})=(n+(m{+}{+})){+}{+}$ by the definition of addition and $(n+(m{+}{+})){+}{+}=((n+m){+}{+}){+}{+}$ using the inductive step. Similarly, on the right hand side we have $((n{+}{+})+m){+}{+}=((n+m){+}{+}){+}{+}$ using the definition of addition. Thus, both sides are equal to each other and we have ~~close~~ closed the induction.

As a particular corollary of the above two lemmas we see that $n{+}{+}=n+1$ (why?)

Proof.
We have, $(n{+}{+})+0=(n+0){+}{+}=n{+}{+}$
$n+1=n+(0{+}{+})=(n+0){+}{+}=n{+}{+}$.

Thus, $n{+}{+}=n+1$.

Proposition. Addition is commutative. For any natural numbers n and m, $n+m=m+n$.

Proof.
We shall use induction on n, keeping m fixed.

- We start with $n+0$ as the base case. By definition of addition $0+n:=n$ and from the above lemma $n+0=n$.
- We inductively assume
  $$m+n=n+m$$
- We would like to show that
  $$(m{+}{+})+n=n+(m{+}{+})$$

On the left hand side, $(m{+}{+})+n=(m+n){+}{+}$ using the definition of addition. From the above lemma, on the RHS, we have — $n+(m{+}{+})=(n+m){+}{+}$. From the inductive step, $m+n=n+m$. So, $(m+n){+}{+}=(n+m){+}{+}$ from axiom 3.

Proposition. Addition is associative.
For any natural numbers a, b, c, we have
$(a+b)+c = a+(b+c)$.

Proof.
We shall use induction keeping a, c fixed and inducting on b.

- We start with $b=0$ as the base case. We are interested to show that
$$(a+0)+c = a+(0+c)$$

LHS
$(a+0)+c$
$= a+c$ since $a+0=a$

RHS
$a+(0+c)$
$= a+c$ by definition of addition $0+c:=c$.

- We assume inductively that
$(a+b)+c = a+(b+c)$
- We would like to show that
$(a+(b{+}{+}))+c = a+((b{+}{+})+c)$.

LHS
$(a+(b{+}{+}))+c = ((a+b){+}{+})+c$ since $n+(m{+}{+}) = (n+m){+}{+}$
$= ((a+b)+c){+}{+}$ by definition of addition

RHS
$a+((b{+}{+})+c) = a+((b+c){+}{+})$
$= (a+(b+c)){+}{+}$

But, $(a+b)+c = a+(b+c)$ from the inductive assumption. Hence, both sides equal each other and we can close the induction.

Because of this associativity we can write sums such as $a+b+c$ without having to worry about which order the numbers are being added together.

Now, we develop a cancellation law.

Proposition Cancellation Law.
Let a, b, c be natural numbers, such that $a+b = a+c$.
Then, we have $b=c$.

Note that we cannot use subtraction or negative numbers yet to prove this proposition, because we have not developed these concepts yet. In fact, this cancellation law is crucial in letting us define subtraction and integers later on in this text, because it allows for a sort of virtual subtraction, even before subtraction is officially defined.

Proof
We prove this by induction on a.
- We consider $a=0$ as base case. We would like to show that if $0+b=0+c \Rightarrow b=c$.

LHS
$0+b=b$

RHS
$0+c=c$

So, $b=c$.

- We inductively assume that if $a+b=a+c$, then $b=c$.

- We now have to prove the cancellation law for $a{+}{+}$.
In other words, we assume that
$$(a{+}{+})+b=(a{+}{+})+c$$
$$\Leftrightarrow (a+b){+}{+}=(a+c){+}{+}$$
$$\Leftrightarrow a+b=a+c \quad \text{since two equal numbers have the same successor.}$$
$$\Leftrightarrow b=c \quad \text{using the inductive assumption.}$$

This closes the induction.

We now discuss how addition interacts with positivity.

Definition (Positive natural numbers). A natural number is said to be positive iff it is not equal to 0.

Proposition. ~~A natural number n is said to be positive~~
If a is positive and b is a natural number, then $a+b$ is positive. (and hence $b+a$ is also positive)

Proof
We use induction on b (keeping a fixed).
If $b=0$, then $a+b=a+0=a$, which is positive so this proves the base case. We inductively assume, that if a is positive and b is a natural number, $a+b$ is positive.
Then, $a+(b{+}{+})=(a+b){+}{+}$, which cannot be zero because of axiom 3, and is hence positive. This closes the induction.

Corollary. If a and b are natural numbers such that $a+b=0$, then $a=0$ and $b=0$.

Proof
Suppose for the sake of contradiction $a\neq 0$ and $b\neq 0$.
If $a\neq 0$, then a is positive and hence $a+b=0$ is positive by the above proposition. But, this is a contradiction. ~~If~~ Similarly, if $b\neq 0$ then b is positive and again $a+b=0$ is positive, a contradiction. Thus, a & b both must be zero.

Lemma. Let a be a positive number. Then, there exists exactly one natural number b such that $b{+}{+}=a$.

Proof
Suppose there are two distinct numbers b, b' such that $b{+}{+} = a$ and $b'{+}{+} = a$ and $b \neq b'$.
since, $a = a \Rightarrow b{+}{+} = b'{+}{+}$.
Invoking axiom 2, we have if $n \neq m$, then $n{+}{+} \neq m{+}{+}$.
The contrapositive of this statement is: if $n{+}{+} = m{+}{+}$, $n = m$.
So, $b = b'$. But, this contradicts our assumption.
Hence, there is only one number b, such that $b{+}{+} = a$.

Once we have a notion of addition, we can begin defining a notion of order.

Definition. Ordering of Natural numbers.
Let n and m be natural numbers. We say that $n \geq m$ or $m \leq n$, if and only if we have $n = m + a$ for some natural number a. We say that n is strictly greater than m, and write $n > m$ or $m < n$, iff $n \geq m$ and $n \neq m$.

Thus, for instance $8 > 5$, because $8 = 5 + 3$ and $8 \neq 5$. Also, note that $n{+}{+} > n$ for any n (since $n{+}{+} = n + 1$ and $n{+}{+} \neq n$); thus there is no largest natural number n, because the next number is still larger.

Proposition. Basic properties of order for natural numbers.
Let a, b, c be natural numbers. Then,
(a) Order is reflexive. $a \geq a$.
(b) Order is transitive. if $a \geq b$ and $b \geq c$, then $a \geq c$.
(c) Order is anti-symmetric. if $a \geq b$ and $b \geq a$ then $a = b$.
(d) Addition preserves order. $a \geq b$ if and only if $a + c \geq b + c$.
(e) $a < b$ if and only if $a{+}{+} \leq b$.
(f) $a < b$ if and only if $b = a + d$ for some positive number d.

Proof.
(a) As $a = a + 0$, by the definition of order, $a \geq a$.
(b) Suppose $a \geq b$ and $b \geq c$.
Therefore $a = b + k$ for some natural number k.
And $b = c + l$ for some natural number l.
Thus $a = c + l + k$
since $l + k$ is a natural number, $a \geq c$.
(c) Suppose $a \geq b$ and $b \geq a$.
Then $a = b + c$ and $b = a + d$.
$\Leftrightarrow$ $a = a + c + d$
$\Leftrightarrow$ $c + d = 0$. By cancellation law.
Thus, both $c = 0$ and $d = 0$.
Hence, $a = b$.

(d) Addition preserves order.
$\Rightarrow$ direction.
$a \geq b$
$\therefore$ $a = b + k$ for some natural number k.
By using the cancellation law
$a + c = b + c + k$ for some natural number k.
$\therefore$ $a + c \geq b + c$.
$\Leftarrow$

(e) $a < b$ if and only if $a{+}{+} \leq b$.

suppose $a < b$.
$\therefore$ $b = a + k$ and $b \neq a$.
If $k = 1$, then $b = a + 1$, that $a{+}{+} = b$.
If $k > 1$, then $k = 1 + l$, that is $b = a + 1 + l$
so, $b \geq a{+}{+}$ or $a{+}{+} \leq b$.

(f) ($\Rightarrow$ direction).
(1) If $a < b$, then $a = b + d$ and $a \neq b$.
Assume that $d = 0$. Then, $a = b$.
We have a contradiction.
so, d must be a positive number.

($\Leftarrow$ direction).
suppose $a = b + d$ for some positive number d.
Assume that $a = b$.
so, $a = a + d$.
By the cancellation law, $d = 0$.
Thus, we have a contradiction.
$\therefore$ $a = b + d$ and $a \neq b$.
so, $a < b$.

proposition (Trichotomy of order for natural numbers).
Let a and b be natural numbers. Then, exactly one of the following statements is true: $a < b$, $a = b$, $a > b$.

Proof
This is only a sketch of the proof. The gaps will be filled in the problems.

First, we show that, we cannot have more than one of the statements $a < b$, $a = b$, $a > b$ holding at the same time. If $a < b$ then $a \neq b$ by definition, and if $a > b$ then $a \neq b$ by definition. If $a < b$ and $a > b$ then $a = b$, a contradiction. Thus, no more than one of the statements is true.

Now, we show that atleast one of the statements is true. We keep b fixed and induct on a. When $a = 0$, we have $0 \leq b$ for all b, because $b = 0 + k$ for some natural number k. so, we have either $0 = b$ or $0 < b$, which proves the base case. Now, suppose we have proven the proposition of a, and now we prove the proposition for $a{+}{+}$. From the trichotomy for a, there are three cases: $a < b$, $a = b$ and $a > b$. If ~~$a < b$~~, then ~~$a{+}{+} \leq$~~ If $a > b$, then $a{+}{+} > b$. If ~~$a = b$~~, since $a = b + k$ (for some positive k and) so $a{+}{+} = (b + k){+}{+} = b + (k{+}{+})$. Thus, $a{+}{+} > b$. If $a = b$, then $a{+}{+} > b$, since $a = b$ implies $a{+}{+} = b{+}{+}$, $a{+}{+} = b + 1$ and thus $a{+}{+} > b$. Now, suppose $a < b$. Then $a{+}{+} \leq b$, by the last proposition. Therefore, $a{+}{+} < b$ or $a{+}{+} = b$, and in either case we are done. This closes the induction.

The properties of order allow one to obtain a stronger version of the principle of induction.

Multiplication.

In the previous section, we have proven all the basic facts that we know to be true about addition and order. To save space and avoid belaboring the ~~obv~~ obvious, we will now allow ourselves to use all rules of algebra concerning addition and order that we are familiar with, without further comment. Thus, for instance we may write things like $a+b+c = c+b+a$ without supplying any further justification. Now, we introduce multiplication. Just as addition is iterated increment operation, multiplication is iterated addition.

Definition. (Multiplication of Natural numbers)
Let m be a natural number. To multiply zero to m, we define $0 \times m := 0$. Now, suppose inductively we have defined how to multiply n to m. Then, we can multiply $n{+}{+}$ to by defining ~~m~~ $(n{+}{+}) \times m := (n \times m) + m$.

Thus, for instance, $0 \times m = 0$, $1 \times m = (0 \times m) + m = m$, $2 \times m = 0 + m + m$, $3 \times m = 0 + m + m + m$. etc. By induction, one can easily verify that the product of two natural numbers is a natural number.

Lemma. The product of two natural numbers is a natural number.

Proof. We use induction on n. Let m be a fixed natural number.

(I) $0 \times m := 0$.
 0 is a natural number.

(II) We inductively assume that $n \times m$ is a natural number.

(III) We are interested to show that $(n{+}{+}) \times m$ is also a natural number. By definition,

$(n{+}{+}) \times m = (n \times m) + m$.
$(n \times m)$ is a natural number from the inductive assumption.
m is a natural number.
The sum of two natural numbers is a natural number.

This closes the induction.

Lemma. Multiplication is commutative. Let n, m be natural numbers. Then, $n \times m = m \times n$.

Proof.
We prove some elementary facts about multiplication and use them in the proof.

(a) For any natural number n, $n \times 0 = 0$.

(I) We use induction on n.
 $0 \times 0 := 0$ by definition.

(II) We inductively assume that
 $n \times 0 = 0$.

(III) We are interested to show that $(n{+}{+}) \times 0 = 0$.
 By definition, $(n{+}{+}) \times 0 = (n \times 0) + 0$
 $= 0 + 0$ since $n \times 0 = 0$ from assumption
 $= 0$ by definition of addition.

This closes the induction.

(b) Show that $n \times (m{+}{+}) = (n \times m) + n$

I. $m \times 0 = 0$.

II. Assume that $n \times (m{+}{+}) = (n \times m) + n$.

III. We are interested to prove that
$$(n{+}{+}) \times (m{+}{+}) = ((n{+}{+}) \times m) + (n{+}{+}).$$

The left-hand side can be simplified as,
$$\begin{aligned}(n{+}{+}) \times (m{+}{+}) &= (n \times (m{+}{+})) + (m{+}{+}) && \text{Definition of multiplication} \\ &= (n \times m) + n + (m{+}{+}) && \text{From what we assumed} \\ &= (n \times m) + (n+m){+}{+}.\end{aligned}$$

The right-hand side can be simplified as,
$$\begin{aligned}((n{+}{+}) \times m) + (n{+}{+}) &= (n \times m) + m + n{+}{+} && \text{Definition of multiplication} \\ &= (n \times m) + (m+n){+}{+} && \text{Property of addition} \\ &= (n \times m) + (n+m){+}{+} && \text{Addition is commutative.}\end{aligned}$$

So, both the sides are equal to each other. This closes the induction.

(c) Show that $n \times m = m \times n$.

(I) $0 \times m := 0$
$m \times 0 = 0$

II. We assume that $n \times m = m \times n$.

III. We are interested to show that $(n{+}{+}) \times m = m \times (n{+}{+})$.

The left hand side can be simplified as:
$$(n{+}{+}) \times m = (n \times m) + m.$$

The right hand side can be simplified as:
$$m \times (n{+}{+}) = (m \times n) + m.$$

From the induction assumption $n \times m = m \times n$.
Hence, both the sides are equal.

This closes the induction.

We will now abbreviate $n \times m$ as nm and use the usual convention that multiplication takes precedence over addition, thus for instance $ab \times c$ means $(a \times b) + c$, not $a \times (b+c)$.

Lemma (Natural numbers have no zero divisors). Let n, m be natural numbers. Then, $n \times m = 0$ if and only if atleast one of n, m is equal to zero. In particular, if n and m are both positive then nm is also positive. (Hint: prove the second statement first).

Proof.

(I) Claim. $1 \times m$ is positive if m is positive.
$1 \times m := m$.
As m is positive, $1 \times m$ is positive.

(II) We inductively assume that $n \times m$ is positive if and only if both n and m are positive.

(III) Claim. $(n++) \times m$ is positive iff both n and m are positive.
$$(n++) \times m := \underbrace{(n \times m)}_{\text{positive}} + \underbrace{m}_{\text{positive}}$$
The sum of two positive numbers is positive.

This closes the induction.

Proposition (Distributive Law).
For any natural numbers a, b, c, we have
$a(b+c) = ab + ac$
$(b+c)a = ba + ca$

Proof.
Since multiplication is commutative, we only need to show the first identity $a(b+c) = ab + ac$. We keep a and b fixed and use induction on c.

Let's prove the base case $c = 0$.
The left side is $a(b+0) = ab$.
The right side is $ab + a0 = ab$.
So, we're done.

Now, let us suppose inductively that
$a(b+c) = ab + ac$.

Let us prove that
$a(b + (c++)) = ab + a(c++)$
The left hand side becomes
$a((b+c)++) = a(b+c) + a = ab + ac + a$.
The right hand side becomes
$ab + ac + a$.

Both sides are equal. This closes the induction.

Proposition. Multiplication is associative. For any natural numbers a, b, c, we have $(a \times b) \times c = a \times (b \times c)$.

Proof.
We induct on c, while keeping a, b fixed.

(I) In the base case, $c = 0$.
$(a \times b) \times 0 = 0$

And, $a \times (b \times c) = a \times 0 = 0$.

(II) We inductively assume that –

$(a \times b) \times c = a \times (b \times c)$

(III) We are interested to show that –

$(a \times b) \times (c{+}{+}) = a \times (b \times (c{+}{+}))$.

On the left-hand side, we have –
$(a \times b) \times (c{+}{+})$
$= (a \times b) \times c + (a \times b)$

On the right hand side we have –
$a \times (b \times (c{+}{+}))$
$= a \times ((b \times c) + b)$
$= a \times (b \times c) + a \times b$

From the inductive assumption,
$(a \times b) \times c = a \times (b \times c)$.

Proposition. Multiplication preserves order.
If a, b are natural numbers, such that $a < b$, and c is positive, then $ac < bc$.

Proof.
$a < b$ means that $b = a + k$, for some positive number k.
$\therefore bc = (a + k)c$
$\therefore bc = ac + kc$
The product of two positive numbers kc is positive.
$\Rightarrow bc > ac$.

Corollary. Let a, b, c be natural numbers such that $ac = bc$ and c is non-zero. Then, $a = b$.

Remark. Just as earlier we did a virtual subtraction, which will eventually let us define genuine subtraction, this corollary provides virtual division which will be needed to define genuine division later.

Proof.

By trichotomy of order, we have three cases -
$a < b$, $a = b$, $a > b$.
Suppose first that $a < b$, then $ac < bc$ and this is a contradiction.
We can obtain a similar contradiction when $a > b$. Specifically, when $a > b$, it means $a = b + d$ for some positive number d. So, $ac = (b+d)c = bc + dc$. As dc is positive, it implies $ac > bc$. As a result, this too is a contradiction.

So, the only possibility is that $a = b$ as desired.

With these propositions, it is easy to deduce all the familiar rules of algebra involving addition and multiplication, the more primitive notion of increment will ~~fall~~ begin to fall by the wayside and we will see it rarely from now on. In any event, we can always use addition to describe incrementation, since $n{+}{+} = n+1$.

Proposition. (Euclidean algorithm.)
Let n be a natural number and let q be a positive number. Then there exists natural numbers m, r such that
$0 \le r < q$ and $n = mq + r$.

Remarks. In other words, we can divide a natural number n by a positive number q to obtain a quotient m (which is another natural number) and a remainder r (which is less than q). This algorithm marks the beginning of number theory, which is a beautiful and important subject but one which is beyond the scope of this text.

Proof.
We fix q and induct on n.

(I) $0 = 0 \cdot q + 0$. and $0 < q$.

(II) We inductively assume that
$n = qm + r$.

(III) We are interested to show that $n{+}{+}$ can be expressed in the form; some multiple $\times q$ + remainder.

$$n{+}{+} = (qm + r){+}{+}$$
$$= qm + (r{+}{+})$$