Math/CS 120: Intro. to Math	Professor: Padraic Bartlett

Lecture 3: Constructing the Natural Numbers

Weeks 3-4 — *UCSB 2014*

When we defined what a proof was in our first set of lectures, we mentioned that we wanted our proofs to only start by assuming "true" statements, which we said were either previously proven-to-be-true statements or a small handful of **axioms**, mathematical statements which we are assuming to be true. At the time, we "handwaved" away what those axioms were, in favor of using known properties/definitions to prove results! In this talk, however, we're going to delve into the bedrock of exactly "what" properties are needed to build up some of our favorite number systems.

1 Building the Natural Numbers

1.1 First attempts.

Intuitively, we think of the natural numbers as the following set:

Definition. The **natural numbers**, denoted as $\mathbb{N}$, is the set of the positive whole numbers. We denote it as follows:

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

This is a fine definition for most of the mathematics we will perform in this class! However, suppose that you were feeling particularly paranoid about your fellow mathematicians; i.e. you have a sneaking suspicion that the Goldbach conjecture is false, and it somehow boils down to the natural numbers being ill-defined. Or you think that you can prove $P = NP$ with the corollary that $\mathbb{P} = \mathbb{NP}$, and to do that you need to figure out what people mean by these blackboard-bolded letters. Or you just wanted to troll your professors in CCS. Or (more likely) your professor in CCS wanted to troll you, by (say) first asking for the definition of the natural numbers, and then poking holes[1] in your answers.

In these worlds, one might make the following objection:

What does "..." mean?

For example, why is a number like 10^{10} in this set, but not 3.5? What "rule" for defining our set is encapsulated by an ellipsis?

A possible second definition for $\mathbb{N}$, that addresses the above criticism, is the following:

$$\mathbb{N} = \{x \mid \text{We can write } x \text{ as the sum } 1 + 1 + \ldots + 1\text{, for some number of 1's.}\}$$

This kind-of answers what we meant by "..." — $\mathbb{N}$ is the collection of all of the numbers you get by repeatedly adding one to itself — but it replaces it with a new and equally opaque

[1] Slightly paraphrased Terry Pratchett: "Demons were like genies or ~~philosophy~~ mathematics professors - if you didn't word things exactly right, they delighted in giving you absolutely accurate and completely misleading answers."

ellipsis. What does this new "…" mean: how many times are we allowed to add 1 to itself? Can we add it to itself π times?

At this point, it is clear that we should avoid ellipses at all costs. Motivated by this, a hypothetical mathematician might return with the following answer:

$$\mathbb{N} = \{x \mid x = 0, \text{ or there is some y in } \mathbb{N} \text{ such that } y + 1 = x\}.$$

No ellipses! Also, this is a good bit clearer: if we look at the above, we can see that we're definitely describing the set that contains zero, and all the things you get by repeatedly adding one to zero!

However, this would not stop any suspicious student from raising more questions. For example: what *is* zero? What is one? What is addition? Why will repeated addition of one to zero get us to something like 10^{10}, but not 3.5? In general, why isn't this set $\mathbb{R}$: after all, for any $r \in \mathbb{R}$, we can definitely write $r = (r-1)+1$ for some element $(r-1) \in \mathbb{R}$!

At this point, many mathematicians might be tempted to throw their chalk at their audience. If we can't even take things like 0 or 1 for granted, where do we even start? It seems like we have nothing to start with!

…nothing to start with.

$$\Huge \emptyset.$$

1.2 First Axioms

Well. If we have nothing to start with, let's start with nothing. Or, to be very specific, let's start with an axiom: nothing exists[2].

Axiom. (Empty Set Axiom.) There is a set containing no members. In symbols:

$$\exists B \text{ such that } \forall x, (x \notin B).$$

We call this set the empty set, and denote it via the symbol $\emptyset$.

So. We have nothing, or (more formally) we can make a set that contains nothing. This is surely a reasonable place to start: if a hypothetical skeptic is not willing to grant the existence of a set containing zero elements, there is probably not much hope of getting them to believe in a set containing more than zero elements.

From here, what can we do? Well: we have $\emptyset$. We also, one assumes, have the ability to manipulate these sets! We write down a few rules for how this works, that (again) most reasonable people would accept as rules to work with.

[2] Be very careful when parsing this statement

Axiom. (Axiom of Extensionality.) Two sets are equal if and only if they share the same elements. In symbols:

$$\forall A, B\ [\forall z, ((z \in A) \Leftrightarrow (z \in B)) \Rightarrow (A = B)].$$

Axiom. (Axiom of Pairing[3].) Given any two sets A, B, we can make a set having as its members just A and B:

$$\forall A, B\ \exists C\ \forall x[x \in C \Leftrightarrow ((x = A) \wedge (x = B)].$$

If A and B are distinct sets, we write this set C as $\{A, B\}$, for shorthand; if $A = B$, then we write it as $\{A\}$. (Recall that because sets do not contain multiple copies of the same object, we would not have $\{A, A\}$ as a set[4].)

Axiom. (Axiom of Union, simple version.) Given any two sets A, B, we can make a set whose members are those sets belonging to either A or B (or both!) In symbols:

$$\forall A, B\ \exists C\ \forall x[x \in C \Leftrightarrow ((x \in A) \wedge (x \in B)].$$

We write this set C as $A \cup B$, for shorthand.

Sometimes, we will want to take unions of more than two things, or indeed more than finitely many things (which is what we could do by simply repeatedly applying the above union axiom.) This is possible, as given by the following stronger union axiom:

Axiom. (Axiom of Union, full version.) Given any set A, there is a set C whose elements are exactly the members of the members of A. In symbols:

$$\forall A\ \exists C\ [(x \in C) \Leftrightarrow (\exists A'(A' \in A) \wedge (x \in A'))].$$

We denote this set as

$$\bigcup_{A' \in A} A'.$$

On the homework, we have you show that this stronger form of union can be used to get our simpler version!

[3]Slightly tweaked from the standard union axiom, for clarity's sake. See me if you'd like to know the differences between our version and the one used in standard ZFC.

[4]A potential objection one could make here, if one wanted to throw a wrench into the works, is the following: what do we mean by a **set**? The answer, roughly speaking, is "we're **defining** sets with these axioms." In other words: a set is any object that you can get by starting with the empty set and whatever objects that you've defined to exist, and applying our axioms! While there are many axiom systems that mathematicians have came up with, the standard model of set theory, Zermelo-Fraenkel+choice, is by far and away the most popular system. It contains ten axioms; we've listed a few in slightly strange forms here. If you'd like to learn about the others, come and talk to me!

Axiom. (Axiom of Power Set.) Take any two sets A, B. We say that $B \subseteq A$ if and only if every member of B is a member of A: in symbols,

$$(B \subseteq A) \Leftrightarrow (\forall x (x \in B) \Rightarrow (x \in A)).$$

Our axiom is the following claim: there is a set $\mathcal{P}(A)$, whose members are precisely the collection of all possible subsets of A. In symbols:

$$\forall A \; \exists P \; \forall B ((B \subseteq A) \Leftrightarrow B \in P).$$

This is a bit weird, so we offer a few examples to illustrate this. Take the set $A = \{1, 2\}$. Then the power set of A, written $\mathcal{P}(A)$, is the following set:

$$\Big\{\emptyset, \{1\}, \{2\}, \{1, 2\}\Big\}.$$

Similarly, if $B = \{\pi, e, \clubsuit\}$, the power set of B is the following set:

$$\Big\{\emptyset, \{\pi\}, \{e\}, \{\clubsuit\}, \{\pi, e\}, \{\pi, \clubsuit\}, \{e, \clubsuit\}\{\pi, e, \clubsuit\}\Big\}.$$

Using these axioms, we can make the following definition:

Definition. Take any set x. The **successor** of x, written $S(x)$, is defined as the following set:

$$S(x) = x \cup \{x\}.$$

In other words: to form $S(x)$, take the set x. By using pairing, form the set $\{x\}$. By using union, form the set $x \cup \{x\}$: this creates $S(x)$!

To illustrate the process, we calculate $S(x)$ for a few sets that you already know here:

$$x = \{1, 2, 3\} \Rightarrow S(x) = \{1, 2, 3, \{1, 2, 3\}\}.$$
$$x = \mathbb{Q} \Rightarrow S(x) = \mathbb{Q} \cup \{\mathbb{Q}\}.$$
$$x = \emptyset \Rightarrow S(x) = \emptyset \cup \{\emptyset\} = \{\emptyset\}.$$

Formally speaking, that last set is the only one that we can make right now; we know that we have the empty set, and thus we can form $S(\emptyset)$. This is a set containing precisely one element, $\emptyset$. So, for brevity's sake, let's **define** $0 = \emptyset, 1 = S(\emptyset)$! This fixes some of our earlier questions: we now know what 0 and 1 are! We can define more natural numbers using this process:

- $S(1) = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\}$. This has two elements: let's call it 2.
- $S(2) = 2 \cup \{2\} = \{0, 1\} \cup \{2\} = \{0, 1, 2\}$. This has three elements: call it 3.
- $S(3) = 3 \cup \{3\} = \{0, 1, 2\} \cup \{3\} = \{0, 1, 2, 3\}$. This has four elements: call it 4.
- ...

From here, it's tempting to make the following definition for $\mathbb{N}$:

$$\mathbb{N} = \{x \mid x = \emptyset, \text{ or } x = S(y), \text{ for some other } y \in \mathbb{N}\}.$$

However, this is not something we can directly do with our axioms. All we know how to do is pair and take unions: this can get us to any $n \in \mathbb{N}$, but actually getting **all** of the natural numbers at once isn't possible with these rules! Basically, we can make any **finite** number, but getting an **infinitely large set** is impossible!

1.3 More Axioms

To get such a set, we need another axiom! As it stands right now, our axioms only make finite sets: to get to the infinite, we explicitly need to make an assumption that infinite things exist[5]. To state this axiom, we need the following definition:

Definition. A set A is called **inductive** if it satisfies the following two properties:

- $\emptyset \in A$.
- If $x \in A$, then $S(x)$ is also in A.

Axiom. (Axiom of Infinity.) There is an inductive set. In symbols:

$$\exists A \ (\emptyset \in A) \wedge (\forall x \in A, S(x) \in A).$$

This is **close** to what we want: we can now make a set that **contains** the natural numbers! This, however, is not the same as a set that **is** the natural numbers: the set given by the above axiom could have lots of other things in it, beyond the natural numbers! We need new axioms and definitions to deal with this: ones that can deal with infinite things, in particular! We develop these here:

Definition. A formula, you might think, is any expression you can write with $\wedge, \vee, \Rightarrow, \neg, (,), \exists, \forall$ and other relevant symbols, along with corresponding variables. However, at a second glance, this looks like a bad definition: we have things like $\neg((\wedge)\vee) \vee p, r \Rightarrow$ that would be considered "formulas," which are perhaps better regarded as nonsense.

Consequently, we need conditions on being "well-formed." This is a little tedious to get into, but it roughly means that your formula actually corresponds to a mathematical statement of some kind: that is, your parentheses are balanced, you don't have a variable occurring in multiple quantifiers, your and statements take in two variables, and such things. Formally, we define being well-formed for formulas about sets recursively, as follows:

- Given any two variables a, b, the strings $a \in b$ and $a = b$ are both well-formed formulas.
- If ϕ is a well-formed formula, then so is $(\neg\phi)$.
- If ϕ and ψ are well-formed formulas, then so is $(\phi \wedge \psi)$. Similarly, so is $(\phi \vee \psi)$ and $(\phi \Rightarrow \psi)$.
- If ϕ is a well-formed formula and x is a variable, then $(\forall x \ \phi)$ and $(\exists x \ \phi)$ are both well-formed formulas.

Unless otherwise specified, we will drop the "well-formed" claim and simply use the word formula to refer to a well-formed formula. (It also bears noting that we can form formulas about things other than sets; they will look similar to the formulas above, except instead of starting with $a \in b$, $a = b$'s we'd have other sorts of true/false expressions, like $x < y$ or $x|y$.)

[5] See this link for an interesting discussion on why infinity is a useful thing to believe in, amongst other threads on stackexchange.

Definition. We say that a variable in a formula is **free** if it is not referred to by any of the quantifiers, and call it **bound** otherwise. For example, in

$$\forall x(\exists y(z \wedge y))$$

the variables x, y are bound, while the variable z is free.

Note that if a formula has no free variables, it is a mathematical **statement**, as defined earlier in class, and thus is something that can be either true or false!

We care about this concept of "formula" because it describes, in a sense, the kinds of claims we can mathematically make about objects! For example, if we wanted to make a formula that says "the set A has at least three elements," we could simply write

$$\exists x, y, z \ \Big(\neg\big((x = y) \vee (y = z) \vee (x = z)\big)\Big) \wedge \Big((x \in A) \wedge (y \in A) \wedge (z \in A)\Big).$$

This formula claims that there are three objects x, y, z, such that these are all distinct and all members of A. If you wanted to strengthen our formula to the claim "the set A has exactly three elements," we would instead have

$$\exists x, y, z \ \Big(\neg\big((x = y) \vee (y = z) \vee (x = z)\big)\Big) \wedge \Big((x \in A) \wedge (y \in A) \wedge (z \in A)\Big) \\ \wedge \Big(\forall w, (w \in A) \Rightarrow \big((w = x) \vee (w = y) \vee (w = z)\big)\Big).$$

This is the same formula as before, except with a third clause that says "for any fourth element w that is in A, this fourth element is actually equal to one of our earlier three elements x, y, z." In other words, this formula is precisely the claim that A has three elements!

Suppose that we have a formula ϕ with one free variable: for example, suppose we have the formula we just described above for sets that contain exactly three elements, which has one free variable given by A. You can think of this formula as describing a **property** of sets: i.e. every set that this formula holds true for could be thought of satisfying that formula, and every set that this formula holds false for could be thought of as failing that formula.

A reasonable thing to want to do, given any formula, is to find all of the sets out of some collection that satisfy that formula! For example, given a collection of sets, I might want to pick out all of the elements of that set that contain three elements, or that contain some fixed element x, or a bunch of other properties. As it currently stands, our axioms don't let us do this: we can just take unions and pairings!

Let's fix that.

Axiom. (Axiom Schema of Specification.) Take any set A. As well, take any formula ϕ, with free variables in the set $x, y, w_1, \ldots w_n$, such that the symbol B is **not** a variable in ϕ. We can then form the set B of all of the elements in A that "satisfy" ϕ! We write this in symbols below:

$$\forall A \ \forall w_1, \ldots \forall w_n \ \exists B \ \forall x \ [(x \in B) \Leftrightarrow ((x \in A) \wedge \phi))].$$

This is a little weird at first, so we give an example. Suppose that we have two sets A, B. Something we might want to create at some point in time is their **intersection**: that is, the collection of all elements that are members of both A and B. We express the existence of this set as follows:

$$\forall A, B \; \exists C \; \forall x \; [(x \in C) \Leftrightarrow ((x \in A) \wedge (x \in B))].$$

For any two specific sets A, B, we denote this set as $A \cap B$.

Notice that we can extend this to intersections of arbitrarily many sets. Suppose we have any set A, and we want to form the intersection of all of the elements $A' \in A$. We can do this using our axiom as follows:

$$\forall A \; \exists C \; \forall x \; [(x \in C) \Leftrightarrow (\forall A'((A' \in A) \Rightarrow (x \in A'))].$$

We denote this set as

$$\bigcap_{A' \in A} A'.$$

You might notice that we asked in our axiom for something a bit weaker than what you'd naturally think we can do. That is: our axiom said that given any set A and formula ϕ, we can pick out all of the elements of A that satisfy ϕ. However, the **natural** thing to want here is the following: given a formula ϕ, why can't we just pick out all of the things that satisfy ϕ? In other words: why do we have to restrict ourselves to picking elements from within some fixed set A — why not just pick our elements from everything?

As it turns out, there are good reasons for the restriction we've given above: in that if I let you pick out properties from everything, you can create contradictions (which are bad!) To give a specific example: consider the "set" made of all sets that do not contain themselves as an element:

$$S = \{A \mid A \notin A\}.$$

The word set is in quotes above because this is not actually a set we can form with our axioms. While the property $\phi : \not(A \in A)$ is a property we can write, the elements of the collection S above aren't restricted to the elements of any specific set!

Because of this, we get some rather unfortunate side-effects. Consider the following natural question: is $S \in S$? Well: if $S \in S$, then it would be a set that contains itself. Consequently, this would make S not an element of itself, as S is only made out of sets that do not contain theirselves. In other words: we have a contradiction!

Therefore, we must have $S \notin S$. But this also causes a problem: because S is made up precisely of those sets that do not contain theirselves, and $S \notin S$, we would have $S \in S$! Another contradiction.

Therefore, no matter what we do here, we would have a contradiction! The problem, therefore, clearly lies at the start of our argument: S cannot be a set! This is why we ask the axiom of specification to limit itself to the elements of a given set that satisfy a given property: to avoid precisely this kind of self-referential paradox.

1.4 Actually Defining $\mathbb{N}$

From here, we can finally start to define $\mathbb{N}$. Take any inductive set S. Let $\mathbb{N}_S$ be defined as follows:

$$\mathbb{N}_S = \bigcap_{\substack{A \subseteq S, \\ A \text{ is inductive}}} A.$$

Note that because "being inductive" is a formula we can write out, and the collection of all subsets of S is also a set we can form, we can use our specification axiom to form this set! (Fill in details here if you're skeptical.)

Our first claim is that these sets are all the same:

Theorem. Take any two inductive sets S, T, and form the sets $\mathbb{N}_S, \mathbb{N}_T$. Then $\mathbb{N}_S = \mathbb{N}_T$.

Proof. By the Axiom of Extensionality, the two sets $\mathbb{N}_S, \mathbb{N}_T$ are equal if and only if they share the same elements. Proving this is easy: look at the intersection $C = \mathbb{N}_S \cap \mathbb{N}_T$ of our two sets. Notice the following properties of this set C:

1. C is a subset of $\mathbb{N}_S$.
2. Consequently, C is a subset of S.
3. C is an inductive set (the proof of this is on your homework!)
4. By points 2 and 3, we know that because

   $$\mathbb{N}_S = \bigcap_{\substack{A \subseteq S, \\ A \text{ is inductive}}} A,$$

   the set C shows up as one of the inductive sets that we intersected to form $\mathbb{N}_S$. In other words, $\mathbb{N}_S \subseteq C$.

By definition, property 1 above simply says that every element of C is an element of $\mathbb{N}_S$, while property 4 says that every element of $\mathbb{N}_S$ is an element of C. Therefore, by our axioms, these sets are equal, as claimed! The same logic applies to $\mathbb{N}_T$: therefore $\mathbb{N}_S = \mathbb{N}_T$. $\square$

Using this theorem, we are justified in making the following definition for $\mathbb{N}$:

Definition. Take any inductive set S, and form the set $\mathbb{N}_S$. This set is the natural numbers, which we denote as $\mathbb{N}$ (because as shown above, the inductive set S itself does not change what $\mathbb{N}_S$ is, which justifies us in ignoring the S-subscript.)

Woo! Eight pages in and we have the natural numbers. What can we **do** with them?

1.5 Properties of $\mathbb{N}$

Well: as a mathematician, once you've built an object, the first thing you want to do is discover all of its **properties**! The **Peano axioms** are a collection of several such statements:

1. 0, which we defined as the empty set $\emptyset$, is a natural number.
2. If a is a natural number, then $S(a)$ is also a natural number.
3. For any natural number a, $S(a) \neq 0$.
4. For any two natural numbers $a, b \in \mathbb{N}$, if $S(a) = S(b)$, then $a = b$. In other words, $S()$ is an injection.
5. If K is an inductive set, then $\mathbb{N} \subseteq K$.

Properties 1, 2 and 5 are free, by definition; as well, property 3 holds because for any a, $S(a)$ counts a as a member, and thus is not the empty set. The only tricky one is property 4, which we prove using a few propositions:

Proposition. Suppose that a is a natural number, and that b is an element of a: i.e. $b \in a$. Then $b \subseteq a$.

Proof. This is a fun proof structure. Consider the following set S:

$$X = \{a \in \mathbb{N} \mid \forall\ b \in a, \text{ we have } b \subseteq a\}.$$

This set is the collection of all natural numbers that have the property that we want. We want to show that this set actually contains all of the natural numbers: in other words, that $X = \mathbb{N}$!

To do this, we will simply show that this set is an inductive set: in other words, that

- $\emptyset \in X$, and
- if $a \in X$, then $S(a) \in X$ as well.

Because we can form $\mathbb{N}$ by taking any inductive set and intersecting all of its inductive subsets, we could then form $\mathbb{N}$ as a subset of X. Because X is already a subset of $\mathbb{N}$, we would have $X \subset \mathbb{N}$ and $\mathbb{N} \subset X$, which we've shown in an earlier proof implies these sets are equal.

To see that X is inductive, simply note the following:

- Consider any sentence of the form "if *blah* is an element of the empty set, then property foo holds." Because the empty set has no members, the first part of this implication statement is always false. Therefore, there is no way for this implication statement to break; the only way to falsify an implication statement is to find a situation where the premise holds and the conclusion fails, and we've just said that our premise never holds! Consequently, this sentence is **always** true, no matter what foo is.

  In particular, this holds for the sentence "if *blah* is an element of the empty set, then *blah* is a subset of the empty set." Therefore, we have shown that $\emptyset$ is a member of X, as claimed.

- Take the set X, and any element a in X. Construct the set $S(a) = a \cup \{a\}$. We want to show that $S(a) \in X$ holds: in other words, that if we take any element from the set $a \cup \{a\}$, it is a subset of $S(a)$.

  There are two possibilities. We can pick an element b from $a \cup \{a\}$ that is from the left-hand-side of the union, that is an element of a itself. By definition, because $a \in X$, we know that $b \subseteq a$; consequently, we have $b \subseteq a \cup \{a\} = S(a)$ as well! (Prove why this last line follows if you don't see why.)

  Alternately, we could pick an element b from $a \cup \{a\}$ from the right-hand side of the union: that is, we could pick $b = a$. Then $a \subset a \cup \{a\}$! (Again, justify this last line if you don't see why it holds.)

This proves that X is an inductive set, which as we noted above is enough to show that $X = \mathbb{N}$; i.e. that every member of $\mathbb{N}$ satisfies the claimed property. □

We place a similar problem on your homework:

Proposition. Suppose that a is a natural number, and that b is an element of a: i.e. $b \in a$. Then a is not a subset of b: in symbols, $a \not\subseteq b$.

Using these two propositions, we can finally prove the fourth Peano axiom here:

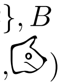
Proposition. For any two natural numbers $a, b \in \mathbb{N}$, if $S(a) = S(b)$, then $a = b$.

Proof. Take any two natural numbers a, b such that $S(a) = S(b)$. Suppose that $a \neq b$; we will show that this contradicts our known properties of $\mathbb{N}$, and thus not a possibility.

Because $S(a) = S(b)$, we know that in particular every element of $S(a)$ is an element of $S(b)$, and vice-versa. So, because $a \in a \cup \{a\} = S(a)$, we have $a \in b \cup \{b\}$; similarly, we have $b \in a \cup \{a\}$.

If $a \neq b$, we would have to have $a \in b$ and $b \in a$. But this contradicts our proposition above: we showed that if $a \in b$, then $b \not\subseteq a$, and therefore that we cannot have $b \in a$ (as that implies that $b \subseteq a$.) Therefore this is an impossible situation to have arrived at, and so our assumption at the start (that $a \neq b$) must be impossible! In other words, we have proven that for any $a, b \in \mathbb{N}$, if $S(a) = S(b)$, then $a = b$. □

From here, we could easily spend a few more weeks making more things rigorous along these lines, like the following.

1. First, notice that given any two sets A, B, we can form their **Cartesian product** $A \times B$, which consists of the collection of ordered pairs (a, b) with $a \in A, b \in B$, For example, if $A = \{1, 2\}, B = \{$ , $\}$, their Cartesian product $A \times B$ would be the collection $\{(1,$$), (2,$$), (1,$$), (2,$$),\}$.

   How do we make this kind of set with our axioms? Well: first, make the following definition: the ordered pair (x, y) will simply be shorthand for the set $\{\{x\}, \{x, y\}\}$. In other words, to specify an ordered pair, we will simply specify the two elements in the ordered pair, along with which element is "first." Note that if $x = y$, this simplifies down to $\{\{x\}\}$.

Now suppose we have a set A. How do we get all of the ordered pairs of elements from A? Well: look at the power set of the power set of A, i.e. $\mathcal{P}(\mathcal{P}(A))$. Elements of this collection consist of sets of subsets of A! So: write a formula that asks for the following:

- We want to only pick out a set B of subsets of A if it has at least one element in it and at most two elements in it.
- If B has one element, that element should be a set containing one element.
- If B has two elements, one of them should be a one-element subset, the other should be a two-element subset, and the only element in the one-element subset should be a member of the two-element subset.

This is clearly something we can write a formula for (see the homework!), and will let us pick out the collection of all ordered pairs of elements of A: in other words, $A \times A$!

For two different sets A, B, simply use the construction above on the set $A \cup B$, and add a final condition on your formula that asks that the "first" element of your pair is in A, and that the second element of your pair is in B. This constructs $A \times B$.

2. With the Cartesian product formed, we can make the notion of a **relation** rigorous. A **relation** R on a Cartesian product $A \times B$ is simply a subset of the elements of $A \times B$: you can think of R as simply a way of saying that certain pairs of elements are related (i.e. they're in R, i.e. R labels them as "true") and that other pairs are not (i.e. they're not in R, i.e. R labels them as "false.")

   You know many examples of relations:

   - Equality (=), on any set S you want, is a relation; it says that $x = x$ is true for any x, and that $x = y$ is false whenever x and y are not the same objects from our set. From the set perspective, this is just the relation $R = \{(x, x) \mid x \in S\}$.
   - "Mod n" ($\equiv \mod n$) is a relation on the integers: we say that $x \equiv y \mod n$ is true whenever $x - y$ is a multiple of n, and say that it is false otherwise.
   - "Less than" (<) is a relation on many sets, for example the real numbers; we say that $x < y$ is true whenever x is a smaller number than y (i.e. when $y - x$ is positive,) and say that it is false otherwise.
   - "Beats" is a relation on the three symbols (rock, paper, scissors) in the game Rock-Paper-Scissors. It says that the three statements "Rock beats scissors," "Scissors beats paper," and "Paper beats rock" are all true, and that all of the other pairings of these symbols are false.

3. A particularly famous example of a relation is a **function**! A function from a set A to a set B is simply a relation on $A \times B$ with the following properties:

   - Every element A is related to some element B. (That is, our function is defined on every element in its domain.)
   - No element in A is related to two elements in B. (That is, our function is well-defined: it doesn't send an element to two different places.)

For example, the function $f(x) = x^2$ on the reals, in set notation, would look like the following:

$$\{(x, x^2) \mid x \in \mathbb{R}\}.$$

4. In mathematics, a common way to define a function is via **recursion**, which is when you define a function by giving it

   - A handful of base cases, for which the function is explicitly defined, and
   - A set of rules that tell you how to reduce any other input to the base case.

   For example, the Fibonacci sequence,

   $$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$$

   is defined recursively via the rules

   - $f(0) = 0, f(1) = 1$, and
   - $f(n+1) = f(n) + f(n-1)$.

   The **recursion theorem** in set theory says that the above method is a valid way to define a function: in other words, giving a set of recursive rules **does** create a function!

5. Addition: using the recursion theorem, we could define addition on the natural numbers recursively as follows:

   - For any $n \in \mathbb{N}$, $n + 0 = 0$.
   - For any $n, m \in \mathbb{N}$ where $m \neq 0$, $n + m = S(n) + P(m)$, where $P(m)$ denotes the "precursor of m," i.e. the natural number such that $S(P(m)) = m$.

6. Similarly, we could define multiplication recursively via addition:

   - For any $n \in \mathbb{N}$, $n \cdot 0 = 0$.
   - For any $n, m \in \mathbb{N}$ where $m \neq 0$, $n \cdot m = n + (n \cdot P(m))$.

7. We could also define a relation $<$ on the natural numbers, by setting $n < m$ if and only if $n \in m$.

Finally, with all of this built up, we can list a number of properties that the natural numbers satisfy with respect to these properties:

- **Closure(+)**: $\forall a, b \in \mathbb{N}$, we have $a+b \in \mathbb{N}$.
- **Identity(+)**: $\exists 0 \in \mathbb{N}$ such that $\forall a \in \mathbb{N}$, $0 + a = a$.
- **Commutativity(+)**: $\forall a, b \in \mathbb{N}, a + b = b + a$.
- **Associativity(+)**: $\forall a, b, c \in \mathbb{N}, (a + b) + c = a + (b + c)$.
- **Closure(·)**: $\forall a, b \in \mathbb{N}$, we have $a \cdot b \in \mathbb{N}$.

- **Identity($\cdot$)**: $\exists 1 \in \mathbb{N}$ such that $\forall a \in \mathbb{N}$, $1 \cdot a = a$.
- **Commutativity($\cdot$)**: $\forall a, b \in \mathbb{N}, a \cdot b = b \cdot a$.
- **Associativity($\cdot$)**: $\forall a, b, c \in \mathbb{N}, (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- **Antireflexivity($<$)**: $\forall a \in \mathbb{N}, a \not< a$.
- **Antisymmetry($<$)**: $\forall a, b \in \mathbb{N}$, exactly one of ($a < b$, $a = b$,$b < a$) holds.
- **Transitivity($<$)**: $\forall a, b, c \in \mathbb{N}$, if $a < b$ and $b < c$, we have $a < c$.
- **Well-Ordering($<$)**: Any subset of natural numbers has a least element.
- **Add. Order($<, +$)**: $\forall a, b, c \in \mathbb{N}$, if $a < b$, then $a + c < b + c$.
- **Distributivity**: $(+, \cdot)$: $\forall a, b, c \in \mathbb{N}, (a + b) \cdot c = (a \cdot c) + (b \cdot c)$

In the interests of time and sanity, we won't prove or go through these properties or proofs, as it would take us a long while!

Instead, next week, we're going to instead talk about a natural extension of the natural numbers: the **integers**!