Monday, March 4

How do you rigorously prove two sets have the same cardinality?

Formatting note: from now on, $A \approx B$ will denote that A and B have the same cardinality.

Propositions: they're little theorems! And also true or false statements! There are also conjectures (guesses) and corollaries (which have short proofs, as they're results of other theorems).

Anyways, here's a proposition: $\mathbb{Z}_{\geq -2} \approx 4\mathbb{Z}_{>0} - 1$.

Intuitively, we can draw the sets:

$$\mathbb{Z}_{\geq -2} = \{-2, -1, 0, 1, 2, \ldots\}$$

$$4\mathbb{Z}_{>0} - 1 = \{3, 7, 11, 15, 19, \ldots\}$$

It looks like there's a way to match these up (map -2 to 3, -1 to 7, 0 to 11, and so on). However, that's not enough to prove the proposition: we need a function.

To make this a formal proof, we need $f: \mathbb{Z}_{\geq -2} \to 4\mathbb{Z}_{>0} - 1$, a function such that for all b in $4\mathbb{Z}_{>0} - 1$, there exists a unique a in $\mathbb{Z}_{\geq -2}$ such that $f(a) = b$. Secretly, there are three things we have to prove, though:

1. We need to construct $f: \mathbb{Z}_{\geq -2} \to 4\mathbb{Z}_{>0} - 1$ and prove that it's a function.
2. We need to check that everything in $4\mathbb{Z}_{>0} - 1$ is an output of f. (Any f satisfying this is called "surjective.")
3. We need to ensure that distinct inputs into f always produce distinct outputs. (Any f satisfying this is called "injective.")

Now let's prove the proposition!

Step 1: we need a function.

$f: \mathbb{Z}_{\geq -2} \longrightarrow 4\mathbb{Z}_{>0} - 1$

What about $n \longmapsto 4n+11$?

This looks promising (-2 is sent to 3, -1 is sent to 7, 0 is sent to 11, and so on), but does it prove the proposition?

(Brief aside: when trying to do something like this, it's always helpful to write down a function, then try to show it's correct.)

This is a function! For any n, f produces exactly one output (being $4n+11$).

Is $4n+11$ an element of $4\mathbb{Z}_{>0}-1$?

Yes: $4n+11 = 4(n+3)-1 \in 4\mathbb{Z}_{>0}-1$, as $n \geq -2$, so $n+3 \geq 1 > 0$, so $n+3 \in \mathbb{Z}_{>0}$. //

↖ This just indicates that the step is over.

Step 2: Is f surjective?

It's time to introduce the wishful thinking bubble!

Scratchwork: Given a random element of $4\mathbb{Z}_{>0}-1$, we want it to be an output of f, i.e. we want $4n-1 = f(x) = 4x+11$, i.e. $4x+11 = 4n-1 \Leftrightarrow x = n-3$.

Proof time! Pick an arbitrary element from $4\mathbb{Z}_{>0}-1$. It can be written as $4n-1$ with $n \in \mathbb{Z}_{>0}$. Then $n-3 > -3$ and $n-3 \in \mathbb{Z}$, so $n-3 \in \mathbb{Z}_{\geq -2} \Rightarrow f(n-3) = 4(n-3)+11 = 4n-1$. ∎ Thus f is surjective. //

(Where did $n-3$ come from? Our wishful thinking bubble! We don't need to justify its existence in our actual proof. We can just choose it, as we know it'll have a nice outcome!)

Step 3: Is f injective?

Want: $x \neq y \Rightarrow f(x) \neq f(y)$, i.e. $f(x) = f(y) \Rightarrow x = y$. $f(x) = f(y) \Rightarrow$

$4x+11 = 4y+11 \Rightarrow x = y$.

(This is rather similar to when we showed two ~~guys~~ people wouldn't get sent to the same room in the Hilbert Hotel problem!)
Proof time! Suppose $f(x)=f(y)$. Then $4x+11=4y+11 \Rightarrow x=y$. //
All three portions have been proved! Q.E.D.
Let's do some injective-surjective examples.

① $f: \mathbb{Z}_{>0} \times \mathbb{Z}_{>0} \longrightarrow \mathbb{Z}_{>0}$
$(h, n) \longmapsto 2^h 3^n$

Is f injective? Yes! (We proved this already—see the Hilbert Hotel example.)
Is f surjective? No! For example, $5 \in \mathbb{Z}_{>0}$, but 5 is never an output of f.

② $g: \mathbb{Z}_{>0} \to \mathbb{Z}_{\geq 0}$ defined by $g(n)$ is the exponent of the largest power of 2 that divides n.

Is g surjective? Yes! $g(2^n)=n$.
Is g injective? No! $g(12)=g(4)=2$.
Next time, we'll prove a badass theorem!