

## Composing Functions and Three Axioms for Integers

Is it possible to have a collection of functions which would satisfy axioms like our axioms for integers? Of course it's possible, but how would one do this so that it's useful?

The first order of business is to find a way to combine two functions to get a third. This is done by *composing* two functions.

**Example:** Define  $f: \mathbb{Z}_2 \rightarrow \mathbb{Z}_7^\times$  by  $f(0) = 1$  and  $f(1) = 6$ . Define  $g: \mathbb{Z}_7^\times \rightarrow \mathbb{Z}_6$  by  $g(3^n) = n$ . Note that we have to check that  $g$  is well-defined!

The composition  $g \circ f$  has domain  $\mathbb{Z}_2$  and codomain  $\mathbb{Z}_6$ . The function values are:

$$g \circ f(0) = g(1) = g(3^6) = 6, \quad g \circ f(1) = g(6) = g(3^3) = 3.$$

**NOTICE!!!** It's quite possible, even likely, that you can only compose two functions one way. In the above example,  $g \circ f$  makes sense, but  $f \circ g$  doesn't! Even if you can compose them either way, the resulting compositions are most likely *not* the same function!

**Example:** Define  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  by  $f(x) = 2x$  and define  $g: \mathbb{Z} \rightarrow \mathbb{Z}$  by

$$g(x) = \begin{cases} 0 & \text{if } x \text{ is even,} \\ 1 & \text{if } x \text{ is odd.} \end{cases}$$

Since the image of  $f$  is the even integers,  $g \circ f(x) = 0$  for any integer  $x$ . But  $f \circ g(1) = 2$ , for instance, so  $f \circ g$  can't be the same function as  $g \circ f$ .

So now that we have a way to combine two functions to get a third (at least when the codomains and domains match up alright), what about those axioms?

Do all functions have an inverse? The answer (you've already seen it in your math career) is no.

Look at the function  $f: \mathbb{Z} \rightarrow \mathbb{N}$  defined by  $f(x) = x^2$ , for example. If  $g \circ f$  is supposed to be the identity function on  $\mathbb{Z}$ , what should  $g(4)$  equal?

We can get around that problem by making sure  $f$  is *one-to-one*.

So let's take a one-to-one function from  $\mathbb{N}$  to  $\mathbb{N}$ :  $f(x) = x^3$ . Now if  $f \circ g$  is the identity function on  $\mathbb{N}$  what should  $g(2)$  equal?

So  $f$  must also be *onto* in order to have an inverse.

Suppose  $S$  is a non-empty set. Then the collection of one-to-one and onto functions  $f: S \rightarrow S$  form a “number system” of sorts. We can combine any two such functions by taking their composition, giving us another such function. This would take the place of  $+$  on  $\mathbb{Z}$ . Like addition of integers, it is associative, there is an identity, and everything has an inverse. *Unlike* addition of integers, composition of two functions is not generally commutative.

In other words, we’ve concocted a “number system” which satisfies the first three of our axioms for integers.