

Functions, Ordering and Congruence: Mathematical Relations

So far in this class we've seen how the ordering of the integers by $<$ makes them rather special. We've also seen how congruences behave much the same way as equality.

Of course, by now all of you have some familiarity with functions, at least functions on real numbers.

All three of these things are particular types of mathematical *relations*. Technically speaking, a relation is just a subset of ordered pairs. But what, technically speaking, is an ordered pair? It's an element of the cartesian product of two sets. But what in the world is **that**? It seems like an infinite decent into a morass of definitions.

Starting in the late 1800's, there was a great effort to view all of mathematics as, ultimately, statements about sets. The goal was to remove all ambiguity and prove all of mathematics was consistent. The pursuit of this goal was interesting in and of itself, though the goal was never attained (for terribly interesting reasons, as it turned out). However, it is true that essentially everything we do in abstract algebra can be written in the language of sets, and this does make things fairly unambiguous.

Definition: Suppose A and B are non-empty sets, with $x \in A$ and $y \in B$. Then the ordered pair (x, y) is defined to be $\{\{x\}, \{x, y\}\}$. The cartesian product $A \times B$ is defined to be the set of all ordered pairs (x, y) where $x \in A$ and $y \in B$.

Notice how this definition gives us what we really wanted all along: an ordered pair is just two things with one “first” and the other “second.” It isn’t too difficult to show that the ordered pair (x, y) is equal to the ordered pair (u, v) if and only $x = u$ and $y = v$. (It’s also an excellent example of how one must be very careful with definitions.)

Definition: Suppose A and B are non-empty sets. A function f from A to B is a subset of the cartesian product $A \times B$ which satisfies the following property: there is at most one element $(x, y) \in f$ for every element $x \in A$. The subset of A consisting of all x where $(x, y) \in f$ for some $y \in B$ is called the *domain* of f . The corresponding subset of B consisting of all y ’s is called the *image* (or sometimes the *range*) of f . The entire set B is called the *codomain*.

Notice how this definition is slightly different than the definition in the textbook. This one is a little handier since one can define functions without having to specifically state the domain. That is more of an issue in other fields, though, which explains the choice made by the authors. If we ever in this class run into a situation where the set A isn’t the domain, I’ll be sure to mention it. If not, just assume A is the domain.

We are most used to defining functions via a formula or rule which assigns to elements x in the domain a particular element y of the codomain. That's especially true when the domain is infinite, for example, with $f: \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = x^2$.

Quite often, however, we'll be considering finite domains. In such a case, it may be simpler to just explicitly write all the elements of f .

Example: Define $f: \mathbb{Z}_6 \rightarrow \mathbb{Z}_7^\times$ by

$$\begin{aligned} f([0]_6) &= [1]_7, & f([1]_6) &= [3]_7, & f([2]_6) &= [2]_7, \\ f([3]_6) &= [6]_7, & f([4]_6) &= [4]_7, & f([5]_6) &= [5]_7 \end{aligned}$$

Technically speaking, this function f is the set of ordered pairs

$$\{([0]_6, [1]_7), ([1]_6, [3]_7), ([2]_6, [2]_7), ([3]_6, [6]_7), ([4]_6, [4]_7), ([5]_6, [5]_7)\}.$$

The important thing to remember is that each x in the domain has a unique y in the image.

When dealing with formulas for a function, it's crucial that the formula really works, i.e., really defines a function.

For example, let's say we want $f: \mathbb{R} \rightarrow \mathbb{R}$ to be defined so that $f(x)$ is the first digit in the decimal expansion of x . For example, $f(32.675) = 3$. But what is $f(1)$? You may recall from high school that $.\bar{9} = 1$, so is $f(1) = 1$ or is it 9?

Keep this in mind when you want to define functions on \mathbb{Z}_n ; remember there are infinitely many ways to express a congruence class $[a]_n$!

To get our feet wet with this generic notion of function, let's list all the functions from the domain $A = \{1, 2\}$ to the codomain $B = \{a, b\}$.

$$\#1 : \quad f(1) = a, \quad f(2) = a$$

$$\#2 : \quad f(1) = a, \quad f(2) = b$$

$$\#3 : \quad f(1) = b, \quad f(2) = a$$

$$\#4 : \quad f(1) = b, \quad f(2) = b$$

Interesting Exercise: Suppose A has m elements and B has n elements. How many elements are there in the cartesian product $A \times B$? (In other words, how many ordered pairs are there?) How many functions are there with domain A and codomain B ?

How many functions are there from \mathbb{Z}_6 into \mathbb{Z}_7^\times ?