Modular Arithmetic: In Motion – Follow-Up Sheet

Katherine E. Stange, University of Colorado Boulder

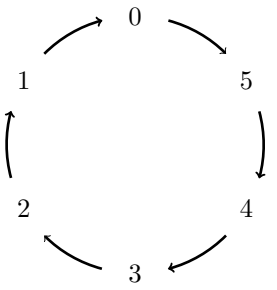
This is a follow-up sheet to accompany the video "Modular Arithmetic: In Motion".

1 Additive dynamics

Each element of $\mathbb{Z}/n\mathbb{Z}$ (the possible residues modulo n) has an *additive action*. For example, 5 *acts additively on* 4 modulo 6, taking 4 to $4+5 \equiv 3 \pmod 6$, which we can draw as an arrow diagram:

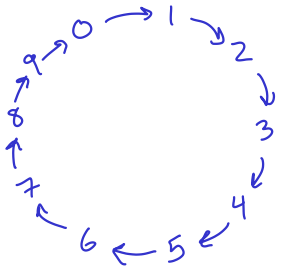
$$4 \xrightarrow{+5} 3$$

Here's a full diagram of the additive action of 5 on $\mathbb{Z}/6\mathbb{Z}$. We call this a *dynamical portrait*:

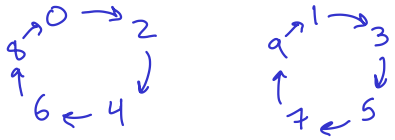


By contrast, here's the full diagram of the additive action of 2 on $\mathbb{Z}/6\mathbb{Z}$:

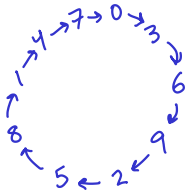
1. Draw the additive action of 1 modulo 10 (i.e. the dynamical portrait of "+1" modulo 10).



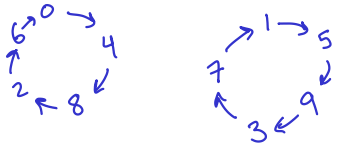
2. Draw the additive action of 2 modulo 10 (i.e. the dynamical portrait of "+2" modulo 10).



3. Draw the additive action of 3 modulo 10 (i.e. the dynamical portrait of "+3" modulo 10).



4. Draw the additive action of 4 modulo 10 (i.e. the dynamical portrait of "+4" modulo 10).



5. Draw the additive action of 5 modulo 10.

6. Draw the additive action of 3 modulo 9.

7. Draw the additive action of 9 modulo 9.

8. Explain why additive dynamics pictures never have two different arrows pointing out of the same place. (Recall this from the video; one sentence suffices.)

The arrows represent the value of a function. On one input, a function has one output. (only one)

9. Consider the function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by $f(x) = x + a$ for any fixed $a \in \mathbb{Z}/n\mathbb{Z}$. Prove that this is bijective by using the definition of injectivity and surjectivity. A well-chosen sentence or two suffices for each.

Injectivity: If $f(x_1) = f(x_2)$ then $x_1 + a \equiv x_2 + a \pmod{n}$, so $x_1 \equiv x_2 \pmod{n}$.

Surjectivity: Let $y \in \mathbb{Z}/n\mathbb{Z}$. Then $f(y - a) = (y - a) + a = y$.

10. Explain why additive dynamics pictures never have two different arrows pointing to the same place. (Recall this from the video; one sentence suffices.)

We've just shown $f(x) = x + a$ is injective. But two arrows pointing to the same place is a failure of injectivity.

11. Explain why additive dynamics pictures always have at least one arrow pointing to each integer. (Recall this from the video; one sentence suffices.)

We just showed $f(x) = x + a$ is surjective.
But no arrows pointing to an integer is a failure of surjectivity.

12. Consider a function $f : A \to A$, where A is a finite set. Explain why this function is surjective if and only if it is injective. This is review from basic material about functions, injectivity, surjectivity and bijectivity, so you may have seen this. However, I'd like you to give a proof in a few sentences that is based on considering the number of arrows and points in a dynamical portrait of this function.

If f is surjective, then every point has an arrow in.
So # arrows $\geq$ # points $= |A|$.
But there's exactly one arrow out of each point (since f is a function).
So # arrows $= |A|$. So # arrows = # points.
Therefore there's at most one into each point. So f is injective.
(Converse is similar.)

13. Explain why the fact that there's one arrow in and one arrow out at every point means the pictures must consist of some number of disjoint cycles. (Recall this from the video; give an outline of the steps.)

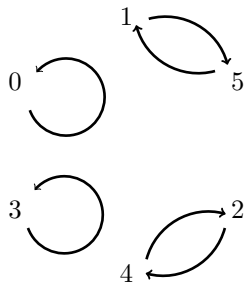
Locally (at each point), we have $\longrightarrow\bullet\longrightarrow$.
So starting at any point we see a chain $\bullet\longrightarrow\bullet\longrightarrow\bullet\longrightarrow\cdots$
It must repeat (since the picture is finite).
It can't repeat at any later point ($\not\longrightarrow\bullet$ not allowed by bijectivity).
So it repeats to the beginning, forming a cycle.  .

2 Multiplicative dynamics

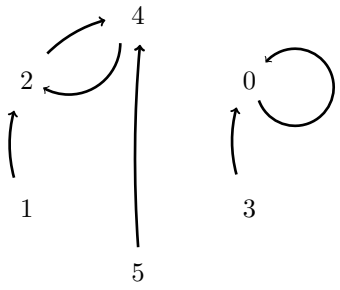
Each element of $\mathbb{Z}/n\mathbb{Z}$ (the possible residues modulo n) has a *multiplicative action*. For example, 5 *acts multiplicatively on* 4 modulo 6, taking 4 to $4 \cdot 5 \equiv 2 \pmod 6$, which we can draw as an arrow diagram:

$$4 \xrightarrow{\cdot 5} 2$$

Here's a full diagram of the multiplicative action of 5 on $\mathbb{Z}/6\mathbb{Z}$:



By contrast, here's the full diagram of the multiplicative action of 2 on $\mathbb{Z}/6\mathbb{Z}$:



As you can see, things are much more interesting for multiplication.

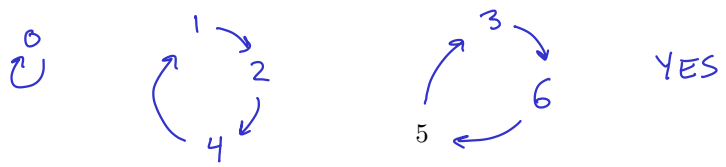
1. In the multiplicative dynamics of a modulo n, sometimes different arrows can point to the same place! Let's call that a *collision*. Give an example from the diagrams above. What does this mean in terms of injectivity/surjectivity of the function $f(x) = ax$?

   1 → 2 → ⋯ ← 4 failure of injectivity @ 2

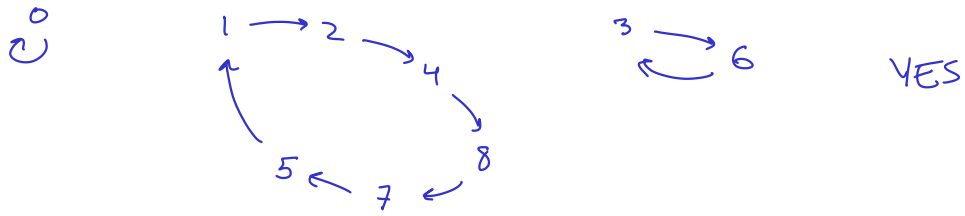
2. It's also possible that some elements have no in-arrows. Give an example from the diagrams above. What does this mean in terms of injectivity/surjectivity of the function $f(x) = ax$?

   1 → ⋯ failure of surjectivity @ 1

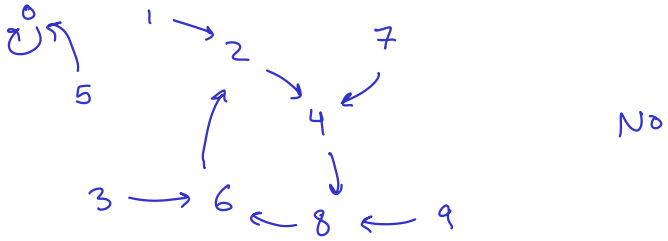
3. Draw the multiplicative dynamics of 2 modulo 7. Is it bijective? Yes/No.



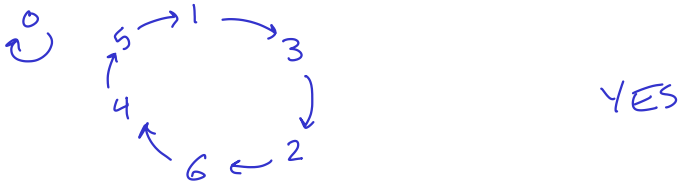
4. Draw the multiplicative dynamics of 2 modulo 9. Is it bijective? Yes/No.



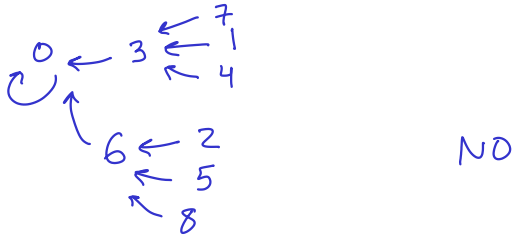
5. Draw the multiplicative dynamics of 2 modulo 10. Is it bijective? Yes/No.



6. Draw the multiplicative dynamics of 3 modulo 7. Is it bijective? Yes/No.



7. Draw the multiplicative dynamics of 3 modulo 9. Is it bijective? Yes/No.



8. Draw the multiplicative dynamics of 3 modulo 10. Is it bijective? Yes/No.