Additive Dynamical Portraits Mod n (Exploration)

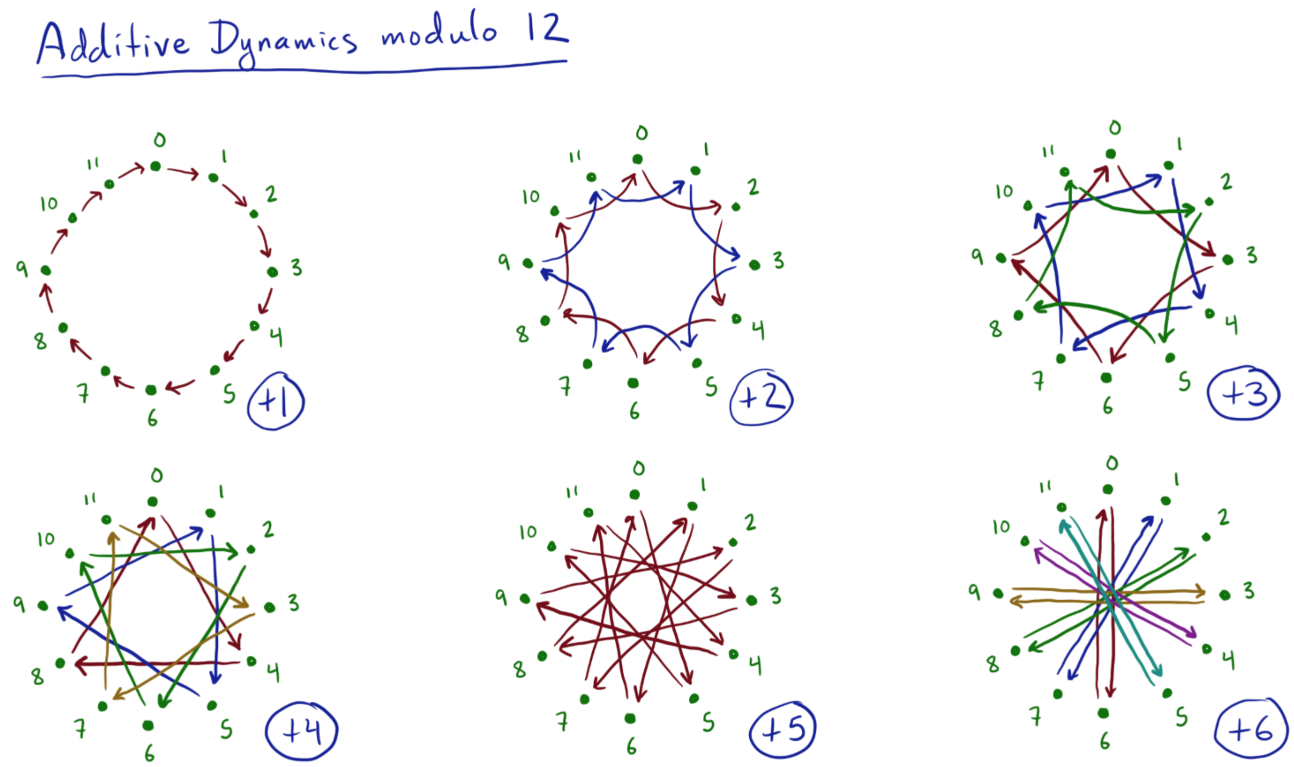
by Katherine E. Stange, University of Colorado Boulder

This is an in-class worksheet exploration. I expect you to have completed the video "Modular Arithmetic: In Motion" and the associated follow-up worksheet. We will use the results from that worksheet.

Main Event

1. Take a look at the examples of multiplicative dynamics you've done, and compare with your groupmates, to catch errors.

2. Here's some more dynamics, of addition modulo 12. Take a look at these carefully and figure out how many cycles there are of what size, in each.



3. For each example you have done, fill in the boldfaced columns in the following table (only the "cycle-size in example" and "# of cycles in example" columns). The examples from the Video Follow-Up worksheet are entered in the table's first two columns, as are the examples modulo 12 drawn above.

a	n	cycle-size conjectured	**cycle-size in example**	# of cycles conjectured	**# of cycles in example**
5	6				
2	6				
1	10				
2	10				
3	10				
4	10				
5	10				
3	9				
9	9				
1	12				
2	12				
3	12				
4	12				
5	12				
6	12				

4. Do more examples if needed, in order to fill in the blanks to make this a conjecture that you, as a group, agree that you believe:

   Conjecture 1. *The number of cycles in the additive dynamics of a modulo n has ____________________ cycles, each of size ____________________.*

   Note: Coming up with this conjecture may take some time and experimentation. Think about divisibility patterns you may see in the table.

5. Fill in the remaining columns in the table and verify that conjecture agrees with experimentation. If it does not, revise your conjecture and start again.

6. Carefully choose three more examples specifically designed to test your conjecture, and add the results to your table. (Farm out the work in your group.)

7. Explain why a cycle starting at b is of size k if and only if k is the smallest positive integer such that $b + ka \equiv b \pmod{n}$.

8. Explain why all cycles in the additive dynamics of a modulo n are of the same size. (Use item 7.)

9. Explain why the size of cycles you stated in Conjecture 1 is the correct size of cycles in the additive dynamics of a modulo n. (Use item 7 with $b = 0$.)

10. Explain the *number* of cycles in your conjecture. How is it related to the size of the cycles?

Further questions

1. Explain why, if a and n are coprime, then the equation $ax \equiv 1 \pmod{n}$ has a solution.

2. The Caesar Cipher can be explained in terms of modular arithmetic. Put the alphabet in bijection with the integers modulo 26:

$$A \leftrightarrow 1, \quad B \leftrightarrow 2, \quad C \leftrightarrow 3, \quad \ldots \quad Z \leftrightarrow 26.$$

   Then, the Caesar Cipher is a encryption shift $f(x) = x + a$ for some a. What is the decryption shift?

3. In the Caeasar Cipher as above given by a shift $x \mapsto x + a$, explain why if we apply the encryption repeatedly, we eventually get back to the original message. How many times must we apply the encryption (as a function of a and n; use what we have learned above)?

4. This question may take some investigation, data collection, conjecturing etc. Consider how to scaffold your investigation. Consider the full set of additive dynamical portraits for $+0, +1, \ldots, +(n-1)$ modulo n. How many of these consist of exactly k cycles?