Modular Dynamics

March 16, 2019

1 Multiplication Tables

Mod 4

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Mod 5

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Mod 6

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Mod 7

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Mod 8

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Mod 9

	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

Mod 10

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

2 Power tables

Mod 4

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	0	0	0	0	0	0	0
3	1	3	1	3	1	3	1

Mod 5

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	4	3	1	2	4	3	1
3	4	2	1	3	4	2	1
4	1	4	1	4	1	4	1

Mod 6

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	4	2	4	2	4	2	4
3	3	3	3	3	3	3	3
4	4	4	4	4	4	4	4
5	1	5	1	5	1	5	1

Mod 7

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	4	1	2	4	1	2	4
3	2	6	4	5	1	3	2
4	2	1	4	2	1	4	2
5	4	6	2	3	1	5	4
6	1	6	1	6	1	6	1

Mod 8

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	4	0	0	0	0	0	0
3	1	3	1	3	1	3	1
4	0	0	0	0	0	0	0
5	1	5	1	5	1	5	1
6	4	0	0	0	0	0	0
7	1	7	1	7	1	7	1

Mod 9

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	4	8	7	5	1	2	4
3	0	0	0	0	0	0	0
4	7	1	4	7	1	4	7
5	7	8	4	2	1	5	7
6	0	0	0	0	0	0	0
7	4	1	7	4	1	7	4
8	1	8	1	8	1	8	1

Mod 10

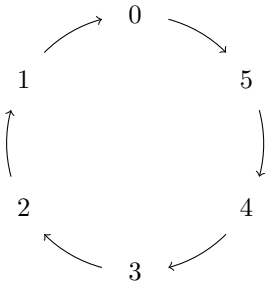
x	x^2	x^3	x^4	x^5	x^6	x^7	x^8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	4	8	6	2	4	8	6
3	9	7	1	3	9	7	1
4	6	4	6	4	6	4	6
5	5	5	5	5	5	5	5
6	6	6	6	6	6	6	6
7	9	3	1	7	9	3	1
8	4	2	6	8	4	2	6
9	1	9	1	9	1	9	1

3 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 $\mathbb{Z}/6\mathbb{Z}$:



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 3 modulo 10.

2. Draw the additive action of 4 modulo 10.

3. Draw the additive action of 5 modulo 10.

4. Draw the additive action of 3 modulo 9.

5. Explain why additive dynamics pictures never have two different arrows pointing out of the same place.

6. Explain why additive dynamics pictures never have two different arrows pointing to the same place.

7. Explain why this means the pictures must consist of some number of disjoint cycles.

8. Explain why the cycles must always be the same size.

9. In the additive dynamics pictures for a modulo n, how many cycles are there? What size are the cycles? Why?

10. Find six moduli n for which the additive dynamics of 6 modulo n is just a single cycle.

11. Find an integer a for which the additive dynamics of a modulo 44 consists of exactly two cycles.

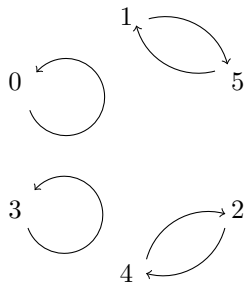
12. Find an integer a for which the additive dynamics of a modulo 44 consists of exactly eleven cycles.

4 Multiplicative dynamics

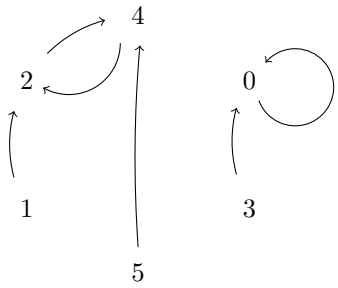
Each element of $\mathbb{Z}/n\mathbb{Z}$ (the possible residues modulo n) has a *multiplicative action*. For example, 5 *acts multiplicatively on* 4 modulo 6, taking 4 to $4 \cdot 5 \equiv 2 \pmod 6$, which we can draw as an arrow diagram:

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

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. Using the diagrams above, compute 2^{100} and 5^{100} modulo 6.

2. Draw the multiplicative dynamics of 2 modulo 7.

3. Draw the multiplicative dynamics of 2 modulo 9.

4. Draw the multiplicative dynamics of 2 modulo 10.

5. Draw the multiplicative dynamics of 3 modulo 7.

6. Draw the multiplicative dynamics of 3 modulo 9.

7. Draw the multiplicative dynamics of 3 modulo 10.

8. Explain why these pictures can never have two different arrows coming out from the same place.

9. 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.

10. Explain why a collision means that a cannot be cancelled modulo n. ('Cancellation' refers to $ax \equiv ay \implies x \equiv y$.)

11. Complete the theorem

    Theorem 1. *The multiplicative dynamics picture of a modulo n has no collisions if and only if*

12. Prove the previous statement.

5 Invertible elements modulo n

In light of the previous section, when considering multiplicative dynamics, it makes sense to restrict to just the invertible elements, i.e. those that are coprime to n.

Definition 1. *The set* $\Phi(n)$ *is the set of integers* $0 \leq x < n$ *such that* $\gcd(x, n) = 1$. *We will write* $\phi(n)$ *for its cardinality.*

1. Compute $\Phi(3)$ and $\phi(3)$.

2. Compute $\Phi(5)$ and $\phi(5)$.

3. Compute $\Phi(7)$ and $\phi(7)$.

4. Compute $\Phi(11)$ and $\phi(11)$.

5. Complete the theorem statement.

   Theorem 2. *When* p *is a prime,* $\phi(p) =$

6. Why is the theorem true?

7. Compute $\Phi(10)$ and $\phi(10)$.

8. Compute $\Phi(15)$ and $\phi(15)$.

9. Compute $\Phi(9)$ and $\phi(9)$.

10. Draw the multiplicative dynamics of 4 modulo 9 on $\Phi(9)$.

11. Draw the multiplicative dynamics of 5 modulo 9 on $\Phi(9)$.

12. Explain why the multiplicative dynamics of $a \in \Phi(n)$ on $\Phi(n)$ cannot have collisions.

13. Explain why the multiplicative dynamics of $a \in \Phi(n)$ on $\Phi(n)$ must consist of disjoint cycles.

14. Explain why the cycles must all be the same size.

15. In the multiplicative dynamics picture of $a \in \Phi(n)$ on $\Phi(n)$, explain why the cycle size must divide $\phi(n)$.

6 The order of an element

Definition 2. *Let $a, n \in \mathbb{Z}$. Let x be the smallest positive integer such that $a^x \equiv 1 \pmod{n}$, if it exists. Then we say x is the* order *of a modulo n.*

1. Compute the order of 2 modulo 7. (You can use tables at beginning of packet if helpful.)

2. Compute the order of 3 modulo 7.

3. Give the full list of elements together with their orders for all elements modulo 7.

4. Here is the famous Fermat-Euler Theorem:

   Theorem 3 (Fermat-Euler)**.** *Let n be a positive integer. Let a be an integer coprime to n. Then the order of a modulo n must divide $\phi(n)$. In particular,*

   $$a^{\phi(n)} \equiv 1 \pmod{n}.$$

   Explain why what you've shown in previous sections actually proves this theorem.

5. Next is the famous Fermat's Little Theorem, which is just the Fermat-Euler Theorem in the case that n is prime (where we have a nice formula for $\phi(n)$). Complete the statement.

   Theorem 4 (Fermat's Little Theorem)**.** *Let p be a prime. Let a be* .
   Then

   $$\equiv 1 \pmod{p}.$$

6. Come up with two examples (of p and a) and test the theorem to see if it holds.

7 A formula for $\phi(n)$

1. Compute $\phi(2)$, $\phi(3)$, $\phi(5)$, $\phi(11)$ and $\phi(10)$, $\phi(15)$, $\phi(22)$.

2. Make a conjecture about $\phi(pq)$ when $p \neq q$ are primes.

3. Can you prove this?

4. What about prime powers? Continue to try to find a formula for $\phi(n)$ in general.