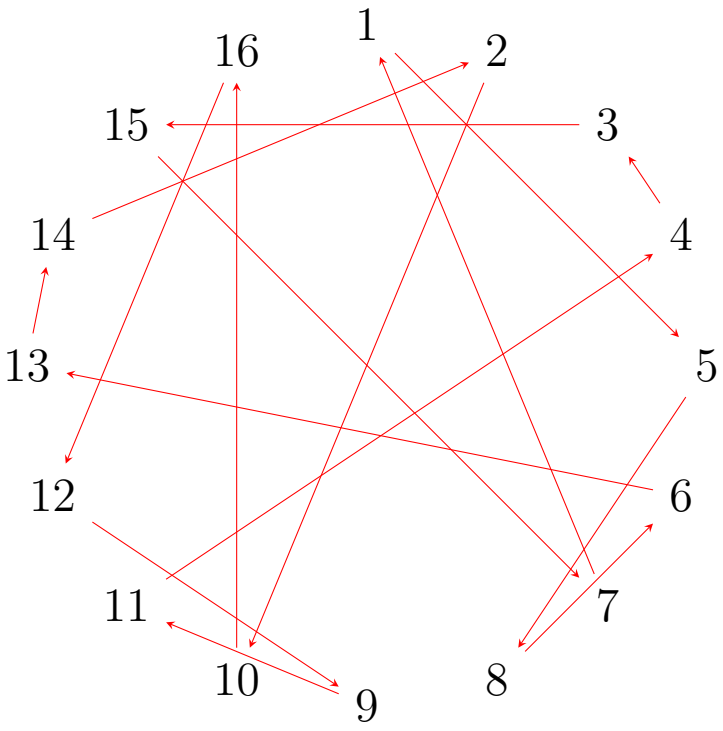
Finding a pattern in modular multiplication

David Gubinelli



Introduction

A famous result in number theory is that if a is a positive integer and p a prime number, then the remainder when a^p is divided by p must be a.

This fact is known as Fermat's little theorem. To avoid having to repeat this confusing sentence every time the theorem is mentioned, from now on I'll use standard modular arithmetic notation:

$$a \equiv b \pmod{n}$$

says that a has remainder b when divided by n. Then the theorem becomes:

$$a^p \equiv a \pmod{p}.$$

"So what ?" you might ask: besides being a nice little party trick for number theorists to impress their friends with, Fermat's little theorem might seem a bit obscure and arbitrary.

However, I will try to present a proof that shows not only how necessary this relationship between prime exponents and prime moduli is, but also how it hints at deeper, more significant results.

I'll be using the theorem as a lens to hopefully show some beautiful patterns in mathematics.

Playing with prime modulo multiplication

Let's think about "least residues". When a positive integer is divided by a prime number p, the possible remainders are

$$0, 1, 2, 3, \ldots, p-2, p-1$$

This is because any larger remainder can be reduced to one of these by subtracting multiples of p.

I'll call this list the "least residues mod p".

These numbers have an interesting behavior when we consider "multiplication mod p" (we multiply the numbers as usual, but then take the result modulo p to obtain a least residue).

Because we consider multiplication, and 0 makes multiplication very boring, from now on I'll exclude 0 from the lists of least residues.

Let's pick p to be a specific prime number, for example 7, and try to observe how least residues mod 7 behave under multiplication:

$$2 \times 5 = 10 \equiv 3 \pmod 7$$

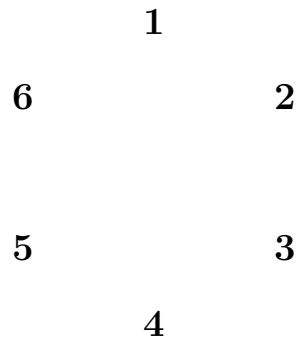
$$4 \times 4 = 16 \equiv 2 \pmod 7$$

$$3 \times 6 = 18 \equiv 4 \pmod 7$$

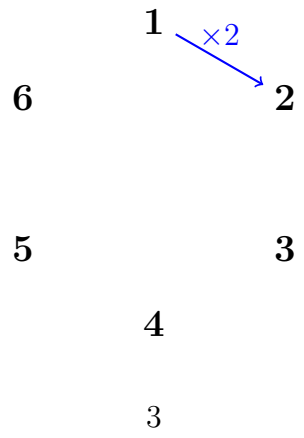
$$\vdots$$

We could continue for a while, but the point is that the pattern of which least residues combine to give which least residue is hard to spot. A good way to visualize it is through a nice circular diagram.

Here is a diagram of the 6 least residues mod 7 (as always, excluding 0).

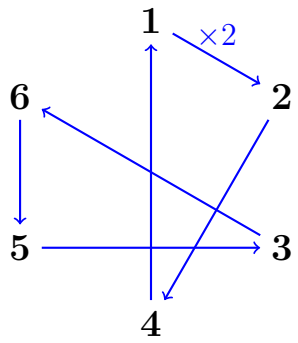


Now, let's represent the action of multiplying by a specific number by a blue arrow. For example, let the blue arrows represent multiplying by 2: the arrow starts at the number we multiply by 2, and ends at the result mod 7.



We can compute the first few arrows. For example, the arrow leaving 1 should obviously go to 2. Then, starting from 2, the arrows should go to $2 \times 2 \equiv 4 \pmod 7$. From 4, the arrow goes to $4 \times 2 \equiv 1 \pmod 7$. The arrows starting at 1 form a cycle, containing 1, 2, and 4. We want our entire diagram to be mapped by the $\times 2$ arrows, so start again at 3 and continue our mapping.

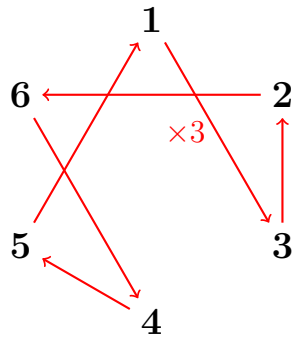
$3 \times 2 \equiv 6 \pmod 7$, and $6 \times 2 \equiv 5 \pmod 7$. Then, $5 \times 2 \equiv 3 \pmod 7$, and we're back to where we started.

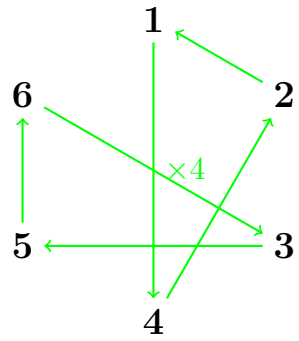


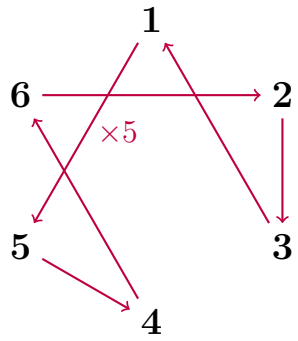
As we can see, this $\times 2$ mapping has formed cycles that have the same number of elements, and that don't overlap with each other (by that I mean the cycles don't share any elements). The first cycle contains 1, 2 and 4, and the second cycle 3, 6 and 5.

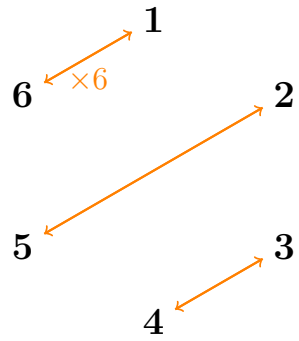
Is this a coincidence ?

If we map other diagrams, for example $\times 3$, $\times 4$, $\times 5$ or $\times 6$:



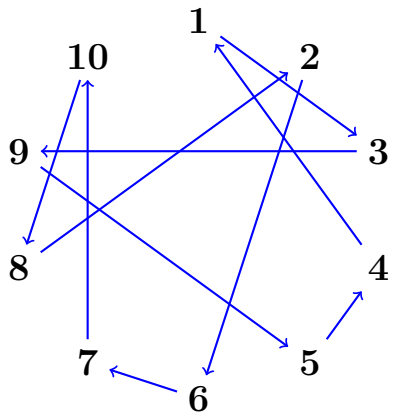


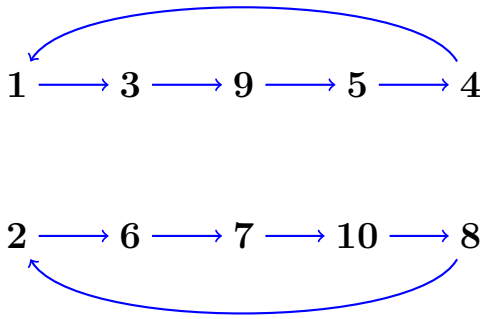




We can see all diagrams contain cycles (1, 2 or 3) that have the same number of elements, and are non-overlapping.

We can choose the least residues (excluding 0) of any prime number, not just 7, and see the same pattern. Here is a diagram of the least residues mod 11, with the arrow ×3. The circular diagram is more cluttered, but the same pattern emerges.



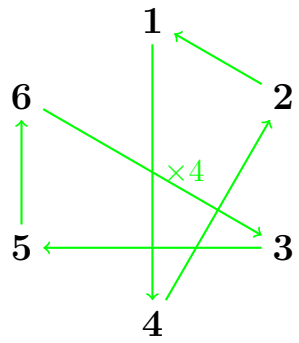


The theorem for least residues

Why do these patterns emerge ?

Cycles are bound to be formed, because there is a finite amount of numbers that can be reached following the arrows.

If we have a cycle that includes 1, but does not include all the numbers in our diagram, say formed by the arrows $\times n$, then we know for some k, the size of the cycle, $n^k \equiv 1 \pmod{p}$. This is because starting at 1, we can follow the $\times n$ arrows k times to end up at 1.



$$1 \times 4 \times 4 \times 4 \equiv 1 \pmod{7}$$

$$4^3 \equiv 1 \pmod{7}$$

Consider another number a of that diagram that is not in the cycle containing 1: because we know $n^k \equiv 1 \pmod{p}$, we know

$$a \times n^k \equiv a \times 1 \equiv a \pmod{p}$$

since multiplication is associative. This represents the fact that following the arrows k times, starting at a, will also end up at a, so a cycle of size k containing a must exist.

We can repeat this argument until every element of the diagram is part of a cycle of size k.

But how do we know the cycles don't overlap?

If they did, some element a would be part of more than one cycle. Start at a and follow the arrows. There is only one result to $a \times n$ (since multiplication is deterministic), and only one least residue that corresponds to $a \times n \bmod p$. Therefore we can only have one arrow leaving a. Following the arrows k times until we return to a gives us one unique cycle. Therefore any element can only be part of a single cycle.

We now know every diagram is split in same-sized, non-overlapping cycles: the cycles partition the diagram.

A direct consequence of this fact is that the total number of elements in the diagram must be an integer multiple of the number of elements in the cycles. So $p-1$ must be an integer multiple of k, the size of the cycles.

$$p - 1 = k \times x$$

for some integer x.

Picture a mapping of the diagram $\times a$, with cycles of size k. We know following the arrows k times brings us back to where we started. Therefore following the arrows $k \times x$ times must also bring us back to where we started, since it represents looping around the cycles x times.

Algebraically, this means:

$$a^{k \times x} \equiv 1 \pmod{p}.$$

And since $p - 1 = k \times x$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Following the $\times a$ arrow one more time:

$$a^p \equiv a \pmod{p}$$

This is almost Fermat's little theorem, because we've only proven it for least residues. We need to show this works for any integer.

We can do that by proving that we are allowed to reduce any integer to its least residue mod p without affecting the result of its multiplication mod p.

We need to show:

$$a^{p-1} \pmod{p} \equiv (a \pmod{p})^{p-1}$$

.

The theorem for all integers

If we have two integers a and b, such that

$$a = a' + k_1 p \equiv a' \pmod{p}$$

$$b = b' + k_2 p \equiv b' \pmod{p}$$

for some integers k_1 and k_2, then

$$ab = (a' + k_1 p)(b' + k_2 p) = a'b' + p(a'k_2 + b'k_1 + k_1 k_2 p) \equiv a'b' \pmod{p}$$

This mess of an equation just shows that applying mod p before or after multiplication does not change the result. This means we can reduce a^{p-1} for any integer a to its least residue to the power of $p - 1$.

Since we've proven the theorem for least residues, and every integer can be reduced to its least residue, the theorem works for any integer.

Generalizing outside of prime moduli

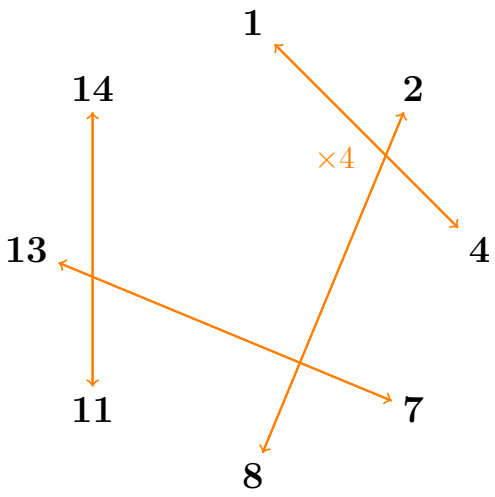
One thing you might have noticed in the previous section is how little we use the restriction that the modulo p must be prime. A natural question to ask is why doesn't this cycle-partitioning-diagram argument work for any modulo n, not just prime?

One problem that we might quickly notice is that if we draw the diagram of least residues mod n (excluding 0) for an integer n, two numbers can multiply mod n to give 0, which is not in our diagram.

For example, even though 3 and 4 are both least residues mod 6, $3 \times 4 = 12 \equiv 0 \pmod{6}$.

We can see that this happens when the numbers we multiply are not coprime to our n, meaning they share a prime factor with n.

But if we restrict the elements of our diagram to just the integers smaller than n that are also coprime with n, we avoid this problem. For example:



Integers smaller than

and coprime to 15

Multiplying mod n any two integers smaller than and coprime to n must also give an integer in the diagram, and therefore we can repeat our argument using cycles:

The arrows will form same-sized, non-overlapping cycles, and therefore the total number of elements in the diagram must be an integer multiple of the number of elements in a cycle.

Since any element to the power of the size of the cycle must be 1, any element to the power of the number of elements in the diagram must also be 1:

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

where $\varphi(n)$ is the number of elements of the diagram, so the integers smaller than and coprime to n. This generalization is called Euler's totient theorem.

Group theory all along

A final question to ask: are these structures that emerged out of our diagrams inherent to modular multiplication, or only a specific example of some larger pattern in algebra?

You might be happy to know that in fact, these cycles partitioning diagrams appear often in mathematics, because they are a property of groups!

If you know some group theory, you may have spotted that by excluding 0, we allowed the least residues to form a group. The cycle containing 1 is a subgroup, the other cycles are its left cosets, and the result we derived is a specific example of Lagrange's theorem!

If you're not familiar with group theory, this conclusion is simply to say that the patterns we've uncovered are only the tip of an iceberg of beautiful structures in mathematics.