Math Circles - Elementary Number Theory - Fall 2023

Week 3 (Nov 29)

So far, we've talked about addition, subtraction, multiplication, and division modulo n. Today, we'll start by talking about exponentiation. We'll start with an example.

Example. *Compute* 2^0, 2_1, 2^2, 2^3, 2^4 *modulo 5.*

Solution.

$$2^0 \equiv 1 \mod 5$$
$$2^1 \equiv 2 \mod 5$$
$$2^2 \equiv 4 \mod 5$$
$$2^3 \equiv 3 \mod 5$$
$$2^4 \equiv 1 \mod 5$$

■

Notice that:

$$2^1 \equiv 2 \cdot 2^0 \equiv 2 \cdot 1 \mod 5$$
$$2^2 \equiv 2 \cdot 2^1 \equiv 2 \cdot 2 \mod 5$$
$$2^3 \equiv 2 \cdot 2^2 \equiv 2 \cdot 4 \mod 5$$
$$2^4 \equiv 2 \cdot 2^3 \equiv 2 \cdot 3 \mod 5$$

Using this strategy, we get that

$$2^5 \equiv 2 \cdot 2^4 \equiv 2 \cdot 1 \mod 5$$

But wait... we already computed $2 \cdot 1 \mod 5$, so we know what this answer is going to be. If we keep going, the answers will keep cycling through the numbers 1, 2, 4, 3, 1, 2, 4, 3, ...

A natural question to ask is whether this will happen for any choice of base g and any choice of modulus n. And the answer is... yes! If we're working modulo n, then the outcome has to be one of the integers $0, \ldots, n-1$. There are only n options, so eventually one of them will have to repeat if we multiply by g enough times. And when this happens, we'll end up in a cycle, like we did in the example.

Let's try another few examples, and see what happens:

Example. *Compute* 2^0, 2_1, 2^2, 2^3, 2^4, 2^5 *modulo 6.*

Solution.

$$2^0 \equiv 1 \mod 6$$
$$2^1 \equiv 2 \mod 6$$
$$2^2 \equiv 4 \mod 6$$
$$2^3 \equiv 2 \mod 6$$
$$2^4 \equiv 4 \mod 6$$
$$2^5 \equiv 2 \mod 6$$

■

Example. *Compute* 5^0, 5^1, 5^2, 5^3, 5^4, 5^5 *modulo 6.*

Solution.

$$5^0 \equiv 1 \mod 6$$
$$5^1 \equiv 5 \mod 6$$
$$5^2 \equiv 1 \mod 6$$
$$5^3 \equiv 5 \mod 6$$
$$5^4 \equiv 1 \mod 6$$
$$5^5 \equiv 5 \mod 6$$

■

In all three examples, we ended up in a cycle. But, our cycles looked different. Our first cycle cycled through all the (non-zero) integers modulo 5. Our second cycle didn't include 1. And our third cycle included 1, but didn't cycle through all the integers modulo 6. Let's brainstorm some of the differences, and other thoughts on these cycles.

Let n be our modulus and let $g \in \{0, \ldots, n-1\}$.

- Picking $g = 1$ (or $g = 0$) will be a very boring cycle.
- It is always the case that $g^0 = 1$.
- Since $g^0 = 1$, if we want to cycle through all elements of $\{1, \ldots, n-1\}$, then we want $g^{n-1} \equiv 1 \mod n$, but we don't want $g^i \equiv 1 \mod n$ for any $i \leq n-1$.
- Since $g^0 = 1$, if it is the case that $g^i \equiv 1 \mod n$ for some $i \leq n-1$, then it must be the case that $i \mid n-1$.

Let's explore a few of these points.

Theorem. *(Fermat's Little Theorem) If* p *is prime then for any* g *in* $\{1, \ldots, p-1\}$*, we have that*

$$g^{p-1} \equiv 1 \mod p.$$

Proof. Let p be prime, and $g \in \{1, \ldots, p-1\}$. First, write out the multiples of g, modulo p:

$$g, 2g, 3g, \ldots, (g-1)g$$

If $rg \equiv sg \mod p$ for some $r \neq s$, then we would have that

$$rg \equiv sg \mod p.$$

But since p is prime, we know from last week that g has an inverse, g^{-1}, so multiplying the above equation by g^{-1} on both sides, we get that

$$rgg^{-1} \equiv sgg^{-1} \mod p$$

and hence that

$$r \equiv s \mod p.$$

But we said that r and s were different, so this can't be true. So, it must be the case that the set of $p-1$ integers

$$\{g, 2g, 3g, \ldots, (p-1)g\}$$

consists of the $p-1$ integers

$$\{1, 2, 3, \ldots, p-1\},$$

in some order. So, if we multiply them all together, we get that

$$g(2g)(3g)\cdots((p-1)g) \equiv 1(2)(3)\cdots(p-1) \mod p.$$

Simplifying this, we get that

$$g^{p-1}(1)(2)(3)\cdots(p-1) \equiv (1)(2)(3)\cdots(p-1) \mod p.$$

We can divide both sides by $(1)(2)(3)\ldots(p-1)$ (since p is prime, this has an inverse modulo p) to get that

$$g^{p-1} \equiv 1 \mod p.$$

■

This theorem can actually be generalized to when p is not prime. Remember Euler's Totient Function, $\Phi(n)$, from Week 1, which counts the number of integers between 1 and n which are relatively prime with n? Well, this is the main reason why we talked about it. First, we'll prove a lemma.[1]

Lemma. *Let* $1 \leq a, b \leq n-1$ *be such that* $\gcd(a,n) = 1$ *and* $\gcd(b,n) = 1$. *Let* $c \equiv ab \mod n$ *such that* $1 \leq c \leq n-1$. *Then* $\gcd(c,n) = 1$.

Proof. We know from Week 1 (by prime factorization) that if $\gcd(a,n) = 1$ and if $\gcd(b,n) = 1$ then $\gcd(ab,n) = 1$. Let $d < 1$ such that $d \mid n$. We need to show that $d \nmid c$. To do this, notice that since $c \equiv ab \mod n$, we can write $ab = c + kn$ for some integer k. Since $d \nmid ab$, we get that $d \nmid c + kn$. But $d \mid kn$, so it must be the case that $d \nmid c$. Since this is true for all divisors d of n, it must be the case that $\gcd(c,n) = 1$. ■

Now, for the actual theorem:

Theorem. *(Euler's Totient Theorem) Let* a *and* n *be integers such that* $\gcd(g,n) = 1$. *Then*

$$g^{\Phi(n)} \equiv 1 \mod n.$$

Proof. Let g and n be integers such that $\gcd(g,n) = 1$, and let $\{a_1, a_2, \ldots, a_{\Phi(n)}\}$ be the set of elements, modulo n, which are relatively prime with n. For the same reasoning as in the proof of Fermat's Little Theorem, each of the elements in the set $\{ga_1, ga_2, \ldots, ga_{\Phi(n)}\}$ are different, and by the lemma above, the set $\{ga_1, ga_2, \ldots, ga_{\Phi(n)}\}$ also consists of all elements, modulo n, which are relatively prime with n (note that the elements might be listed in a different order). So, similarly to the proof of Fermat's Little Theorem, we get that

$$(ga_1)(ga_2)(ga_3)\cdots(ga_{\Phi(n)}) \equiv a_1(a_2)(a_3)\cdots(a_{\Phi(n)}) \mod n.$$

Simplifying this, we get that

$$g^{\Phi(n)}(a_1)(a_2)(a_3)\cdots(a_{\Phi(n)}) \equiv a_1(a_2)(a_3)\cdots(a_{\Phi(n)}) \mod n.$$

We can divide both sides by $a_1(a_2)(a_3)\cdots(a_{\Phi(n)})$ to get that

$$g^{\Phi(n)} \equiv 1 \mod n.$$

■

[1] A *lemma* is a small theorem.