Orders and Euler's Theorem

Friday, March 27

Last time: We conjectured that if p is prime, then for any $a < p$ we have $a^{p-1} \equiv 1 \pmod{p}$. This led to a discussion of the **order** of elements. Here is a summary of what we have so far:

- For any finite group G and any element $g \in G$, we say the **order** of g is the least k such that $g^k = e$ (the identity).

- We also noted that if $\mathrm{ord}(g) = k$ then $g, g^2, g^3, \ldots, g^k$ are distinct elements. Why is this?

$g^m = g^n$ $\quad m<n<k$ $\quad g^3 \cdot g^2 = g^{3+2}$

$g^m g^{-m} = g^n g^{-m}$

$e = g^{n-m}$ $\quad 0<n-m<k$

contradiction

- Since there are k distinct powers of g, we have that the cyclic subgroup generated by g, that is, $\langle g \rangle$ contains exactly k elements.

- Thus the order of the element g is equal to the order of the cyclic subgroup generated by g.

- But Lagrange's theorem tells us that the order of a subgroup must divide the order of the group.

- Thus the order of any element $g \in G$ must divide the order of G.

Now let's continue where we left off.

- Suppose $\mathrm{ord}(g) = k$. What is g^{nk} for any n?

$g^{nk} = (g^k)^n = e^n = e$

$U(7) = \mathbb{Z}_7^*$

$\mathrm{ord}(2) = 3$

Therefore: $g^{|G|} = e$

$|U(7)| = 6$

$2^6 = 1$

- Now consider the group $U(p)$ where p is prime. This is the group of *units* mod p, which means $\{1, 2, 3, \ldots, p-1\}$ (which is a consequence of Bezout's lemma).

$g \in U(p)$

$h \cdot g \equiv 1 \mod p$

$hg = k \cdot p + 1$

$h \cdot g - k \cdot p = 1$

$\gcd(g, p)$

$p-1 = |U(p)|$

- Thus in $U(p)$ we have $g^{p-1} = 1$ for all $g \in U(p)$.
- Therefore $a^{p-1} \equiv 1 \pmod{p}$. This result is called *Fermat's Little Theorem.*

Now what about the non-prime case? Given n, is there a number m such that $a^m \equiv 1 \pmod{n}$ for all a?

$n = 6$

if a and n have a comon factor, then there will be no m.

$2^m \equiv 1 \mod 6$?

But... if a is relatively prime to n... ?

- Working in groups again, we can consider $U(n)$. The elements of this group are precisely the *units* of Z_n, which means those elements relatively prime to n.

$U(6) = \{1, 5\}$

$U(8) = \{1, 3, 5, 7\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

$U(9) = \{1, 2, 4, 5, 7, 8\}$

$g^{|U(n)|} \equiv 1 \mod (n)$

For any $g \in U(n)$

- We will let $\varphi(n)$ denote the *number* of numbers less than n that are relatively prime to n. This is called the **Euler φ-function**.

$\varphi(7) = 6$

$\varphi(9) = 6$

$\varphi(8) = 4$

$\varphi(n) = |U(n)|$

- What do we get if we repeat the same argument as we did for Fermat's Little Theorem?

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

for a relatively prime to n.

This is known as Euler's Theorem.

For Euler's theorem to be useful, we need to understand how the φ function behaves.

- We know that $\varphi(p) = p - 1$ for any prime p. We also will define $\varphi(1) = 1$ (because it will be useful to do so).
- The definition of $\varphi(n)$ is: the number of positive integers less than n that are relatively prime to n. Find $\varphi(n)$ by brute force for some non-prime values of n.
- In particular, find $\varphi(6)$, $\varphi(10)$, $\varphi(14)$, $\varphi(15)$, and $\varphi(21)$. Note that each of these is the product of two primes.
- $\varphi(4) = 2$, $\varphi(6) = 2$, $\varphi(8) =$

$\varphi(10) = ?\ 4$

1, 2, 3, 4, 5, 6, 7, 8, 9, $\cancel{10}$
✓ ✗ ✓ ✗ ✗ ✗ ✓ ✗ ✓

$\varphi(10) = 4$

$\varphi(14) = 6$

$\varphi(22) = 10$

$\varphi(26) = 12$

$26 = 2 \cdot 13$

$\varphi(15) = 8 = 2 \cdot 4$

$\varphi(21) = 12 = 2 \cdot 6$

$\varphi(p \cdot q) = (p-1)(q-1) \leftarrow$

$p \neq q$ primes.