## 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  $a^k = e$  (the identity).
- We also noted that if  $\operatorname{ord}(g) = k$  then  $g, g^2, g^3, \dots, g^k$  are distinct elements. Why is this?

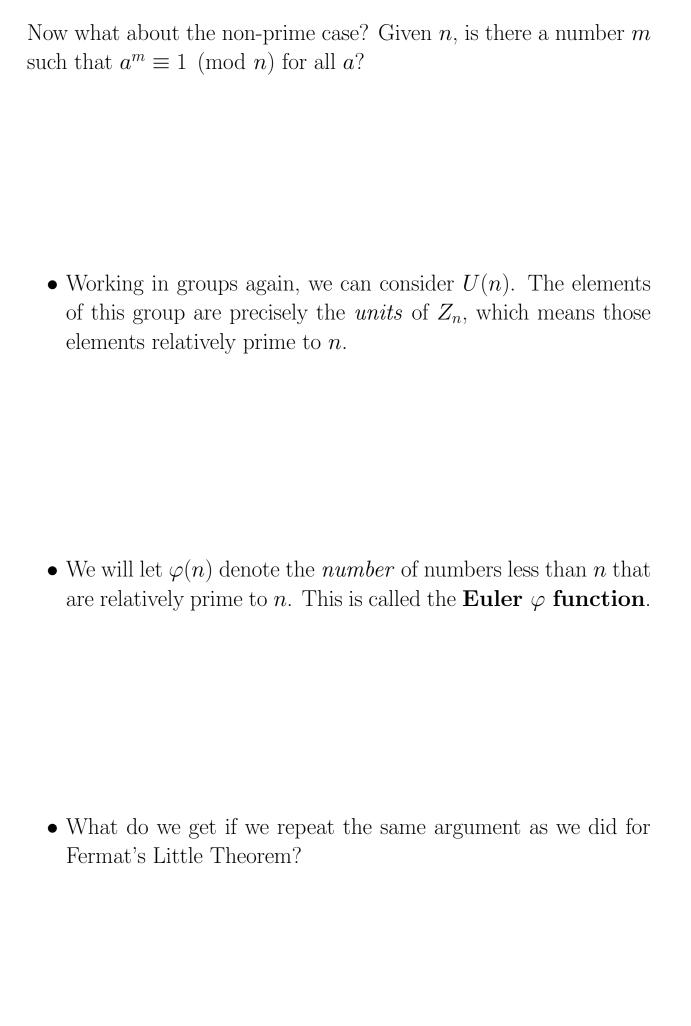
- Since there are k distinct powers of g, we have that the cyclic subgroup generated by g, that is,  $\langle g \rangle$  contains exactly k elements.
- Thus the order of the element g is equal to the order of the cyclic subgroup generated by g.
- But Lagrange's theorem tells us that the order of a subgroup 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  $\operatorname{ord}(g) = k$ . What is  $g^{nk}$  for any n?

• 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).

- 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*.



This is known as Euler's Theorem.

For Euler's theorem to be useful, we need to understand how the  $\varphi$  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.
- $\varphi(4) = 2, \ \varphi(6) = 2, \ \varphi(8) =$