MATH 335 Lecture 20

Chris Camano: ccamano@sfsu.edu

November 1, 2022

Lagranges theorem and associated concequences

Let G be a finite group and H a subgroup of G, then the index of H in G denoted:

$$[G:H]$$

Which is equivilant to the number of left cosets of H in G

$$[G:H] = \frac{|G|}{|H|}$$

In particular the order of H divides the order of G.

1. If G is a finte group and we pick any element in g then $|g|||G|$

   Proof. The order of an element g is equal to the number of elements in the cyclic subgroup generated by g this is to say:
   $$|g| = |<g>|$$
   So by lagranges theorem :
   $$|<g>|||G|$$
   □

2. In a finite group G with $|G| = n$, $g^n = e$ for all $g \in G$

   Proof. let $|g| = d$ then by the previous proof we know that $d|n$
   $$g^n = (g^d)^{\frac{n}{d}} = e^{\frac{n}{d}} = e$$
   Since n over d is an integer by Lagranges theorem: □

3. If G is a group with order p where p is a prime number, then G must be a cylic

Proof. $p \geq 2$ so there is at least one non identity element, ge Consider the subgroup generated by this element:

$$H =< g >$$

Lagranges theorem gives us $|H|||G|$ but the order of G is a prime number, therefore:

$$|H| = 1 \text{ or } p$$

but we said that it cannot be 1 meaning the only possibility is that H has order p so

$$H =< g >= G$$

If the order of G is prime any non identity element is a generator □

Euler's theorem

Suppose a,n , n¿0 are integers that are coprime.
Then :

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

Proof.

$$U(n) = \{[m] : gcd(n,m) = 1\}$$
$$|U(n)| = \phi(n)$$

Then by Collary two if we take a finite group element and raise it to the order we get identity. We can use this since gcd(a,n)=1

$$[a]^{|U(n)|} = [1]$$
$$[a]^{\phi(n)} = [1]$$
$$a^{\phi(n)} \equiv 1 \mod n$$

□

Fermat's Little Theorem

If a prime p does not divide a, this is to say p and a are coprime, then

$$a^{p-1} \equiv 1 \mod p$$

Proof. $a^{\phi(p)} = a^{p-1} \equiv 1 \mod p$ □