Lemma: Properties of Cosets Let H be a subgroup of G, and let $a, b \in G$. Then,

1. $a \in aH$,
2. $aH = H$ if and only if $a \in H$,
3. $aH = bH$ if and only if $a \in bH$,
4. $aH = bH$ or $aH \cap bH = \emptyset$,
5. $aH = bH$ if and only if $a^{-1}b \in H$,
6. $|aH| = |bH|$,
7. $aH = Ha$ if and only if $H = aHa^{-1}$,
8. aH is a subgroup of G if and only if $a \in H$.

Lagrange's Theorem If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of H in G is $|G|/|H|$.

We define the *index* of H in G to be the number of left (right) cosets of H in G. We denote the index by $|G : H|$. A direct consequence of Legrange's theorem is a formula for this as recorded by Corollary 1:

Corollary 1 If G is a finite group and H is a subgroup of G, then $|G : H| = |G|/|H|$.

1. The following corollary is often our most used application of Lagrange's Theorem. Prove it please: (Hint: Remember each element forms a cyclic subgroup. hmm. Which Theorem was that? How was the order related to the order of the element?Which Theorem was that?)

   Corollary 2: In a finite group, the order of each element divides the order of the group.

2. **NOTE:** The converse of this is false! Just because a number divides the order of a group does not guarantee that there exists an element of that order. Prove this by finding a group of order n with divisor k of n, but no element of order k. (Hint: Examples abound in Chapter 5.)

3. In the past the following problem was a little complicated to prove, but Lagrange's theorem and its corollary make it easy: Prove that a group of order 5 is cyclic.

4. Prove the more general version of this problem which is recorded as a Corollary to Lagrange's Theorem:
   Corollary 3 A group of prime order is cyclic.

5. Prove the following Corollaries:
Corollary 4**:** Let G be a finite group, and let $a \in G$. Then $a^{|G|} = e$.(Hint: Use Cor. 2.)

Corollary 5**: Fermat's Little Theorem** For every integer a and every prime p,

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

Note:This is pretty easy using Cor. 4, but there are 2 cases to consider: 1) $gcd(a, p) = 1$, and 2) $gcd(a, p) \neq 1$. Note the second case implies $p \mid a$. Do you see why?

6. Use the ideas in the previous corollaries to quickly find $7^{26} \pmod{15}$ (do not use your calculator program to do it, but you can use it to check if you're correct).

7. Find the last digit of 97^{12345}. (Hint: How does thinking modulo 10 help?)

8. Let a and b be non-identity elements of different orders in a group of order 155. Prove that the only subgroup of G that contains both a and b is G itself.