Lab Notes 2/10/12

I. Operations in a group

Group $\mathbb{Z}^*_p$ | has p-1 elements
| If p is prime, all elements in group have a multiplicative inverse

Definition- a set that has binary operations that are associative, for all elements $a \in G$, there exists the multiplicative inverse, a^{-1}, in G, and has the property of closure.

1. Binary operations
   a. For a (some operation) b, if $a,b \in G$, then $a*b \in G$
2. Multiplicative Inverse
   a. $a \in G$
   b. $\exists a^{-1} \in G$
   c. Such that $a * a^{-1} = I$, where I is the identity(or 1)
3. Closure
   a. All products and sums of elements within the group will still be in the group
   b. EX: G($\mathbb{Z}^*_5$, +) $4+2 \equiv 1$ (Note: there is an implied (mod 5) here)
   c. Multiplication table of a closed group $\mathbb{Z}^*_5$

*	**1**	**2**	**3**	**4**
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

   d. This table is always symmetric along the diagonal

II. Multiplicative Order

Definition of multiplicative order- the smalls k such that $a^k \equiv I (\text{mod } n)$

1. Example for $\mathbb{Z}^*_5$
   a. $4^2 \equiv 1$ (means 2 is the multiplicative order of 4 in this group)
   b. $3^4 \equiv 1$ (4 is the multiplicative order of 3)
2. Suppose $a \in \mathbb{Z}^*_n$ has a multiplicative order k. Show that for any $m \in \mathbb{Z}$, the multiplicative order of a^m is k/gcd(k,m)

   Proof

   (trying to prove $(a^m)^{k/\gcd(m,k)} \equiv 1 (\text{mod } n)$)

   1. Let d = gcd(m,k)

2. k = dk'
3. m= dm'
4. $(a^m)^{k'} = a^{dm'k'} = a^{km'} \equiv (a^k)^{m'}$ (mod n)
5. Since $ord_n(a) = k$ (Note "$ord_n(a)$ means the multiplicative order of a (mod n) is k and this is told from the supposition)
6. For any integer y, if $a^y \equiv 1$(mod n) then k|y.
7. From $a^{mx} \equiv 1$ (mod n) follows therefore k|mx
8. mx = kl for some integer l
9. mx/d = kl/d
10. m'x = k'l
11. Since gcd(m', k') = 1
12. k'|x

III. Quadratic Residue

a. a is a quadratic residue if $a \equiv x^2$(mod n) for some $x \in \mathbb{Z}$
b. Euler Criterion
   i. If a is a quadratic residue (mod p) then $a^{(p-1)/2} \equiv 1$
   ii. If $a^{(p-1)/2}$ is congruent to 1 it is a quadratic residue, if it is congruent to -1, it is not

EX: Show that 3 is a quadratic residue mod 23

1. $3^{(23-1)/2} \equiv 3^{11}$
2. $\equiv 3^3 * 3^3 * 3$
3. $\equiv 3^3 * 3^8$
4. $\equiv 3^3 * 3^5 * 4$
5. $\equiv 4 * 4 * 4 * 9$
6. $\equiv 1$