Notes for 13 Feb (Wednesday)

1 The road so far...

1. Discussed the units and zero divisors of $\mathbb{Z}/m\mathbb{Z}$. Proved that $\mathbb{Z}/m\mathbb{Z}$ is a field iff m is a prime.
2. Defined integral domains and studied the number of roots of linear and quadratic equations over commutative rings.

2 Rings and Fields

Theorem 1. *If R is a* finite *commutative ring, and $a \in R$ is any nonzero element, then a is either a unit or a zero divisor.*

Proof. Suppose a is not a zero divisor. Then consider $\{1, a, \ldots, a^{n-1}\}$ where $n = |R|$. Since a is not a zero divisor (unless $0 = 1$ and hence the entire ring is $R = \{0\}$, in which case the theorem is trivially true) none of the n elements above are 0. Since $R - \{0\}$ has $n - 1$ element, by PHP, there exist $i < j$ such that $a^i = a^j$. Inductively applying the cancellation law (because a is not a zero divisor), $1 = a^{j-i}$ hence, if $a \neq 1$, then a^{j-i-1} is the multiplicative inverse of a. □

So, in a finite commutative ring R such that $m = |R|$, every unit a has a smallest natural $d_a < m$ such that $a^{d_a} = 1$. Such a d_a is called the order of a. For example, in $\mathbb{Z}_4$, $[3]_4^2 = [1]_4$ and hence $[3]_4$ has order 2.

3 Fermat and Eulers' theorems

Since $\mathbb{Z}/m\mathbb{Z}$ is a finite commutative ring, every unit has an order. Also,

Lemma 3.1. *Let $m \geq 2$. Then a and m are coprime iff there exists a $1 \leq t < m$ such that $[a^t]_m = [1]_m$.*

Proof. Indeed, if $[a^t]_m = [1]_m$, then a is a unit and hence is coprime to m. If a and m are coprime, then a is a unit and by the above theorem we are done. □

For example, in $\mathbb{Z}_7$, all nonzero elements are units. $[2]^2 = [4], [2]^3 = [6], [2]^4 = [1]$. So $ord(2) = 3$. $[3]^2 = [2], [3]^3 = [6], [3]^4 = [4], [3]^5 = [5], [3]^6 = [1]$. So $ord(3) = 6$. Now $[4]^2 = [2], [4]^3 = [1] ord(4) = 3$. $[5]^2 = [4], [5]^3 = [6], [5]^4 = [2], [5]^5 = [3], [5]^6 = [1], ord(5) = 6$. $[6]^2 = [1], ord(6) = 2$. The order of an element is quite similar to the lcm. Just like the lcm,

Lemma 3.2. *If e is the order of $[a]_m$, and $[a]^f = [1]$, then e divides f.*

Proof. Suppose $f = eq + r$. Then $[a]^f = [a]^e q[a]^r = [a]^r = [1]$ which means that $r = 0$ because e is the smallest such integer. □

Moreover,

Lemma 3.3. *If $ord([a]_m) = e$, and $d > 0$, then $ord([a]^d) = u = \frac{e}{gcd(d,e)}$.*

Proof. Note that $([a]^d)^u = [1]$. We have to prove that such a u is the smallest. Indeed, if r satisfied $[a]^d r = 1$, then dr is a multiple of e and hence $dr \geq \frac{de}{gcd(d,e)}$ which implies that $r \geq u$. □

Here is an important result that tells us something about the order of all elements of $\mathbb{Z}_p$.

Theorem 2. *(Fermat's little theorem) : $[a]_p^{p-1} = [1]_p$ where p is a prime.*

Proof. Take $[a].[1], [a].[2], \ldots, [a].[p-1]$. If we multiply these togther, we get $[a]^{p-1}[1].[2].[3]. \ldots [p-1]$. Noting that these numbers are all distinct, non-zero, and they are $p-1$ in number, they have to be a permutation of $1, 2 \ldots, p-1$. Thus, $[a]^{p-1}[1].[2]. \ldots = [1].[2] \ldots$ which means that $[a]^{p-1} = [1]_p$. □

Therefore, the order of any element in $\mathbb{Z}_p - \{0\}$ divides $p-1$. (This is a special case of a more general phenomenon.)
For more general $\mathbb{Z}/m\mathbb{Z}$, here is Euler's theorem.

Theorem 3. *Let $\phi(m)$ be the number of numbers $\leq m$ that are coprime to m. Then $[a]_m^{\phi(m)} = [1]_m$ for every unit $[a]_m \in \mathbb{Z}/m\mathbb{Z}$.*

Proof. Let G be the group of units of $\mathbb{Z}/m\mathbb{Z}$. G consists of numbers that are coprime to m. If $[a]_m$ is such a number, consider $[a]_m[1]_m[a]_m[x_2]_m \ldots [a]_m[x_{\phi(m)}]_m$. Clearly this set is a permutation of $[1]_m, [2]_m \ldots$. Therefore their products are equal which means that $[a]_m^{\phi(m)} = [1]_m$. □

Now we need to know how to calculate $\phi(m)$. That is given by the following theorem.

Theorem 4. *1. If p is a prime, $\phi(p) = p - 1$.*

2. If p is a prime, $\phi(p^e) = p^{e-1}(p-1)$.

3. If a and b are coprime, then $\phi(ab) = \phi(a)\phi(b)$.

Proof. Part 3 will be given as a HW. The other two parts are as follows.

1. Clearly, $1, 2 \ldots, p-1$ are coprime to p. Thus $\phi(p) = p - 1$.

2. We induct on e. For $e = 1$ we are done. Assume truth for $1, 2, \ldots, e-1$. $p^{e-1} < a \leq p^e$ is divisible by p iff $a = pb$ where $p^{e-2} < b \leq p^{e-1}$. Therefore, the number of numbers $\leq p^e$ divisible by p are $p^{e-1} - \phi(p^{e-1}) + (p^{e-1} - p^{e-2}) = p^{e-1}$. Thus, $\phi(p^e) = p^e - p^{e-1}$.

□

Actually, Euler's theorem is a special case of a more general theorem (which is itself a special case of Lagrange's theorem).

Theorem 5. *For any element $a \in G$ where G is a commutative group, $a^{|G|} = 1$.*

Proof. Take the set $a.1, a.x_2, a.x_3 \ldots, a.x_{|G|-1}$. This set is simply a permutation of the group. Hence, $a^{|G|} 1.x_2.x_3 \ldots = 1.x_2.x_3 \ldots$. Therefore, $a^{|G|} = 1$. □