Lecture 11

We have seen that any cyclic group is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}/m\mathbb{Z}$ (for some integer m). We will now explore further properties of cyclic groups.

Order of an element

Suppose $G = \langle a \rangle$. Then, a typical element of G is of the form a^k where $k \in \mathbb{Z}$.

Question: What is $\mathrm{ord}(a^k)$?

The answer depends on ord(a).

<u>If ord(a) is not finite</u>, then G is isomorphic to $\mathbb{Z}$.

In this case, any non-identity element has <u>infinite</u> order.

So, now <u>suppose $\mathrm{ord}(a) = m$</u>, where m is a positive integer.

Suppose k is positive.

We consider the sequence

$a^k, a^{2k}, a^{3k}, \ldots\ldots$

The first time 1 will occur in this sequence is at a^{kd}, where kd is the smallest multiple of k which is also a multiple of m.

So $kd = \operatorname{lcm}(k, m)$.

<u>Recall</u> $k \cdot m = \gcd(k,m) \cdot \operatorname{lcm}(k,m)$.

(Prove this!)

So we see that

$$\operatorname{ord}(a^k) = d = \frac{\operatorname{lcm}(k,m)}{k}$$

$$= \frac{m}{\gcd(k,m)}.$$

If k is negative, we can apply this argument to $-k$ to get $\operatorname{ord}(a^{-k}) = \dfrac{m}{\gcd(-k, m)}$

However, $\operatorname{ord}(a^{k}) = \operatorname{ord}(a^{-k})$ and $\gcd(k, m) = \gcd(-k, m)$

So, $\operatorname{ord}(a^{k}) = \dfrac{m}{\gcd(k, m)}$

We have proved:

<u>Theorem 1</u> Suppose $G = \langle a \rangle$ and $\mathrm{ord}(a) = m$, where $m \in \mathbb{Z}$.

Then, $\mathrm{ord}(a^k) = \dfrac{m}{\gcd(k,m)}$

for any integer k.

Note that for any element x of a group, $|\langle x \rangle| = \text{ord}(x)$.

So, we have:

<u>Corollary 1</u> Under the above hypothesis, $|\langle a^k \rangle| = \dfrac{m}{\gcd(k,m)}$.

Corollary 2 Under the above hypothesis, a^k is a generator of $G = \langle a \rangle$ if and only if $\gcd(k, m) = 1$, i.e. $\bar{k} \in U(m)$.

(Recall: $\bar{k} = (k + m\mathbb{Z}) \in \mathbb{Z}/m\mathbb{Z}$.)

More generally, we see that a^k and a^l have the same order $\iff \gcd(k,m) = \gcd(l,m)$.

Now, for a fixed integer k, let $d = \gcd(k,m)$.

Then, $\gcd(d,m) = d = \gcd(k,m)$.

So, $\operatorname{ord}(a^d) = \operatorname{ord}(a^k) = m/d$.

So, $|\langle a^d \rangle| = m/d$.

However, we also see that $a^k = (a^d)^{k/d}$ is an element of $\langle a^d \rangle$.

As $\mathrm{ord}(a^k) = m/d = |\langle a^d \rangle|$, we see that a^k generates the subgroup $\langle a^d \rangle$.

So, we have proved :

<u>Theorem 2</u> Suppose $G = \langle a \rangle$ with $\mathrm{ord}(a) = m \in \mathbb{Z}$. Then, for any $k \in \mathbb{Z}$, $\langle a^k \rangle = \langle a^{\gcd(k,m)} \rangle$.

Now, let d be any divisor of m.

Then, $\langle a^d \rangle$ is a group of order m/d.

On the other hand, if k is any integer, the subgroup $\langle a^k \rangle$ has order m/d if and only if $d = \gcd(k, m)$.

Theorem 2 shows that in that case $\langle a^k \rangle = \langle a^d \rangle$.

Thus, we have proved:

<u>Corollary 3</u> Under the above hypothesis, for any divisor d of m, G has a unique <u>cyclic</u> subgroup of order m/d. It is generated by a^d.

We have proved that if ord(a) is infinite (i.e. if G is isomorphic to $\mathbb{Z}$), then any subgroup of $G = \langle a \rangle$ is <u>cyclic</u>.

What happens if ord(a) is finite?

Theorem 3 Suppose $G = \langle a \rangle$ with $\text{ord}(a) = m \in \mathbb{Z}$. Then, every subgroup of G is cyclic.

Proof: $G = \{1, a, a^2, \dots, a^{m-1}\}$. Let H be a subgroup of G. Suppose $H \neq \{1\}$.

Let $t =$ smallest positive integer such that $t < m$ and $a^t \in H$.

We claim that $H = \langle a^t \rangle$.

Indeed let a^s be in H.

Write $s = tq + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < t$.

Then, $a^r = a^t \cdot a^{-sq} \in H$.

But by the choice of t, this is possible only if $r = 0$.

Thus $a^s \in \langle a^t \rangle$.

Thus $H \subseteq \langle a^t \rangle$.

As $\langle a^t \rangle \subseteq H$, we conclude that $H = \langle a^t \rangle$. //

The group $U(m)$

Recall that the set $U(m)$ is the collection of cosets $a + m\mathbb{Z}$ such that $\gcd(a, m) = 1$. We saw that $U(m)$ is a group under multiplication.

Definition (Euler's φ function)

For any positive integer m, we define $\varphi(m) = |U(m)|$.

Thus, $\varphi(m) =$ number of integers k such that $0 \leq k < m$ and $\gcd(k, m) = 1$.

Easy examples

- If p is a prime number,

  $\varphi(p) = p-1.$

- If p is a prime number and k a positive integer,

  $\varphi(p^k) = p^{k-1}$ (number of integers $\leq p^k$ which are divisible by p)

Theorem 4 Let m, n be positive integers such that $\gcd(m,n)=1$. Then $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

Proof: Let r, s be integers such that $mr + ns = 1$.

We will define a function $f: U(m) \times U(n) \longrightarrow U(mn)$.

Let $\bar{a} \in U(m)$, $\bar{b} \in U(n)$.

Define $f(\bar{a}, \bar{b}) = \bar{x} \in \mathbb{Z}/mn\mathbb{Z}$

where $x = ans + bmr$.

Recall that $\gcd(m, a) = 1$ and $\gcd(m, n) = 1$ by hypothesis.

As $mr + ns = 1$, we also have $\gcd(m, s) = 1$.

So $\gcd(m, ans) = 1$

So $\gcd(m, ans + bmr) = 1$,

i.e. $\gcd(m, x) = 1$.

A similar argument shows

$\gcd(n, x) = 1$.

So $\gcd(mn, x) = 1$, i.e.

$\overline{x} \in U(mn)$.

We need to check that f is well-defined, i.e. we need to see that $\overline{x} = \overline{ans + bmr}$ does not change if we replace a and b by some other elements of $\overline{a} = a + m\mathbb{Z}$ and $\overline{b} = b + n\mathbb{Z}$ respectively.

Suppose $a_1 \equiv a \pmod{m}$

and $b_1 \equiv b \pmod{n}$.

Let $x_1 = a_1 ns + b_1 mr$.

We see that $m \mid a_1 s - as = (a_1 - a)s$

and so $mn \mid a_1 ns - ans$.

Similarly, $mn \mid b_1 mr - bmr$.

So $mn \mid (a_1 ns + b_1 mr) - (ans + bmr) = x_1 - x$.

So $x_1 \equiv x \pmod{mn}$, i.e.
$\overline{x_1} = \overline{x}$.

Thus, f is well-defined.

<u>Claim 1</u> f is one-to-one.

Indeed, suppose $f(\bar{a}_1, \bar{b}_1) = f(\bar{a}_2, \bar{b}_2)$.

Then $mn \mid (a_1 ns + b_1 mr) - (a_2 ns + b_2 mr)$

$(a_1 ns + b_1 mr) - (a_2 ns + b_2 mr)$

$= ns(a_1 - a_2) + mr(b_1 - b_2)$

If m divides this expression,

$m \mid ns(a_1 - a_2)$.

But $\gcd(m, ns) = 1 \Rightarrow m \mid a_1 - a_2$

i.e. $\overline{a_1} = \overline{a_2}$.

Similarly, $\overline{b_1} = \overline{b_2}$.

So f is a one-to-one function.

<u>Claim 2</u> f is onto.

Let $\bar{x} \in U(mn)$.

Then $\gcd(x, mn) = 1$

$\Rightarrow \gcd(x, m) = 1$ and $\gcd(x, n) = 1$.

So $(x + m\mathbb{Z}) \in U(m)$ and $(x + n\mathbb{Z}) \in U(n)$

What is $f(x+m\mathbb{Z}, \ x+n\mathbb{Z})$?

$$xns + xmr = x(ns + mr)$$
$$= x \cdot 1 = x.$$

So $f(x+m\mathbb{Z}, \ x+n\mathbb{Z}) = x + mn\mathbb{Z}$

(i.e. $\bar{x}$).

Thus, f is onto.

This shows that

$f: U(m) \times U(n) \longrightarrow U(mn)$

is a 1-1 correspondence.

Thus $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

Example

$$\varphi(300) = \varphi(2^2 \cdot 3 \cdot 5^2)$$

$$= \varphi(2^2) \cdot \varphi(3) \cdot \varphi(5^2)$$

$$= (2^2 - 2) \cdot (3^1 - 3^0) \cdot (5^2 - 5)$$

$$= 2 \cdot 2 \cdot 20 = 80.$$

Theorem Let m be a positive integer. Let $a \in \mathbb{Z}$ such that $\gcd(a, m) = 1$. Then, $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Proof: $\overline{a} \in U(m)$.

Thus, $\operatorname{ord}(\overline{a}) \mid |U(m)| = \varphi(m)$.

So $\overline{a}^{\varphi(m)} = \overline{1}$, i.e. $a^{\varphi(m)} \equiv 1 \pmod{m}$. //

Corollary (Fermat's Little theorem)

Let p be a prime number.

Let $a \in \mathbb{Z}$. Then:

(1) If $\gcd(a, p) = 1$, then

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

(2) In general $a^p \equiv a \pmod{p}$.

Proof: Hint: $\varphi(p) = p-1$. //