LECTURE 9

(Wednesday OCT. 16, 2019)

$\Rightarrow$: Conversely — assume $a^n = e$. By division w. remainder: Write

$$n = \mathrm{ord}(a)\,t + r, \qquad 0 \leq r < \mathrm{ord}(a).$$

Then

$$a^n = \left(a^{\mathrm{ord}(a)}\right)^t * a^r = e * a^r = a^r$$

— our Hypothesis: $a^n = e$; $a^{\mathrm{ord}(a)} = e$.

— This reads: $a^r = e$. By minimality of $\mathrm{ord}(a)$, r cannot be > 0. Must have $r = 0$. In other words $\mathrm{ord}(a) \mid n$. □

— In particular, when $\mathrm{ord}(a) < \infty$:

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{\mathrm{ord}(a)-1}\}.$$

(this list has no repetitions)

Thus, $\boxed{|\langle a \rangle| = \mathrm{ord}(a)}$.

Def. $(G, *)$ is a CYCLIC group if there's an $a \in G$ s.t. every element of G is a power of a. I.e., if $G = \langle a \rangle$ for some $a \in G$.

Ex $\mathbb{Z}_7^\times = \{[1], [2], [3], [4], [5], [6]\}$

- $\text{ord}[1] = 1$.
- $\text{ord}[2] = ?$. Modulo 7:

  $2^1 \equiv 2 \quad 2^2 \equiv 4 \quad 2^3 \equiv 1$ — shows $\text{ord}[2] = 3$

  $\langle [2] \rangle = \{[1], [2], [4]\}$.
- $\text{ord}[3] = ?$. Modulo 7:

  $3^1 \equiv 3 \quad 3^2 \equiv 2 \quad 3^3 \equiv 6 \quad 3^4 \equiv 4$

  $3^5 \equiv 5 \quad 3^6 \equiv 1$ — shows $\text{ord}[3] = 6$

$\langle [3] \rangle = \{[1], [3], [2], [6], [4], [5]\} = \mathbb{Z}_7^\times$.

so $[3]$ generates $\mathbb{Z}_7^\times$, which is therefore cyclic.

Exc: Complete this for $[4] = [2]^{-1}$ and $[5] = [3]^{-1}$

(ord $[6] = \text{ord}[-1] = 2$)

↑ another generator for $\mathbb{Z}_7^\times$.

Fact ("Primitive Roots")

$\mathbb{Z}_p^\times$ is always cyclic when $p =$ prime.

(found earlier that $\mathbb{Z}_{12}^\times$ is not: All elements have order ≤ 2)

§ Cyclic <u>additive</u> groups:

(1) $\mathbb{Z}$ with $+$. Every $x \in \mathbb{Z}$ is a multiple of 1.

$$x = \underbrace{1+1+\cdots+1}_{x} = x1 \quad (\text{if } x>0)$$

cyclic.

- 1 is a generator
- -1 is a generator.

(2) $\mathbb{Z}_N$ with $+$. Similar.

$$[x] = \underbrace{[1]+\cdots+[1]}_{x} = x[1].$$

cyclic.

- $[1]$ is a generator.

<u>Exc</u>: $[a]$ generates $\mathbb{Z}_N \iff GCD(a,N)=1$.
(additively)

— so $\mathbb{Z}_N$ has N elements, $\varphi(N)$ of which are generators.

Hint:

<u>Order—Formula</u>: $(G,*)$ group. Suppose $ord(a)<\infty$.

Then $\forall n \in \mathbb{Z}$:

$$ord(a^n) = \frac{ord(a)}{GCD(n, ord(a))}$$