LECTURE 13

(Monday OCT. 28, 2019)

$\{1, 3, 5, 9, 15, 45\}$

Ex. Subgroups of $\mathbb{Z}_{45} \longleftrightarrow$ divisors of 45

($45 = 3^2 \cdot 5$ has $(2+1)(1+1) = 6$ divisors > 0)

Six $H \leqslant \mathbb{Z}_{45}$. Four non-trivial ones:

- $|H| = 3$: $\{[0], [15], [30]\} = H_1$

- $|H| = 5$: $\{[0], [9], [18], [27], [36]\} = H_2$

- $|H| = 9$: $\{[0], [5], [10], \ldots\ldots, [40]\} = H_3$

- $|H| = 15$: $\{[0], [3], [6], \ldots, [42]\} = H_4$

inclusions among them:

$H_1 \subseteq H_3$

$H_1 \subseteq H_4$

$H_2 \subseteq H_4$

$(H_1 = H_3 \cap H_4)$

Thm. $(G,*)$ cyclic group of size $|G|=N$.
Let $d|N$ any (positive) divisor. Then:

$$\boxed{G \text{ has } \underline{\text{exactly}}\ \varphi(d) \text{ elements of order } d.}$$

[$d=N$: G has $\varphi(N)$ generators ← above generalizes this result].

PROOF. Let $H \leq G$ be the subgroup of size $|H|=d$ (it's cyclic $=\langle a^{\frac{N}{d}}\rangle$ if $G=\langle a\rangle$)

Suppose $x\in G$ has $\mathrm{ord}(x)=d$. Then $|\langle x\rangle|=d$

so by uniqueness of H, must have $\langle x\rangle = H$.

— in particular $x\in H$ and x is a generator for H.

Conversely, if $x\in H$ generates H, $\mathrm{ord}(x)=d$.

Conclude:

$$\left\{\begin{matrix}\text{elements of } G\\ \text{of order } d.\end{matrix}\right\} = \underbrace{\left\{\begin{matrix}\text{generators}\\ \text{of } H\end{matrix}\right\}}_{\substack{\text{KNOW this has } \varphi(d)\\ \text{elements since } H\\ \text{is cyclic of size } d.}}.$$

$\square$

<u>Corollary</u> ("φ-sum formula")

$$\sum_{d|N} \varphi(d) = N$$

all divisors >0.

PROOF. $\mathrm{ord}(x)$ divides N ($x \in G =$ any cyclic group of size N)
(by order-formula)

Let $X_d = \{x \in G : \mathrm{ord}(x) = d\}$. Then:

$$G = \bigcup_{d|N} X_d \quad \text{(disjoint union)}.$$

previous <u>Thm.</u>

Now count: $N = |G| = \sum_{d|N} |X_d| = \sum_{d|N} \varphi(d)$ $\square$

<u>EX</u>: $N = p^r$. Here

$$\sum_{d|N} \varphi(d) = \sum_{n=0}^{r} \varphi(p^n) = 1 + \sum_{n=1}^{r} (p^n - p^{n-1}) = p^r$$

— can turn this into an alternate proof of COR. using that $N \mapsto \sum_{d|N} \varphi(d)$ is a "<u>multiplicative</u>" function.

Primitive Roots mod p: $\mathbb{Z}_p^\times$ cyclic. "field"
(p = prime)

(in general a polynomial f over $\mathbb{Z}_p$ has $\leq \deg(f)$ roots)

— can prove this, assuming:

(★) FACT: $x^d \equiv 1 \pmod p$ has $\leq d$ solutions mod p.

EX $(d=2)$: $x^2 \equiv 1\ (p) \iff p \mid (x+1)(x-1)$

$\iff p \mid (x+1)$ or $p \mid (x-1)$

$\iff x \equiv \pm 1\ (p)$

— using p prime ("Euclid's Lemma").

fails if p not prime (composite): Saw $x^2 \equiv 1 \pmod{12}$ has 4 solutions 1, 5, 7, 11.

(also $x^3 \equiv 1 \pmod{12} \Rightarrow x \equiv 1$)

Thm. $\mathbb{Z}_p^\times$ cyclic.

PROOF. Let $\forall d \mid \phi(p) = p-1$:

$$N_d = \#\{x \in \mathbb{Z}_p^\times : \operatorname{ord}(x) = d\}$$

CLAIM: $N_d = 0$ or $N_d = \phi(d)$

— by margin note

(and obviously $\sum_{d \mid p-1} N_d = p-1$.)

• NOTE: By "Fermat's Little Theorem": $a^{p-1} \equiv 1 \pmod p$ (shown later..) we know $\operatorname{ord}(x) \mid (p-1)$

Why? Suppose $N_d \neq \emptyset$, i.e. $\exists x \in \mathbb{Z}_p^\times$ of order d.

Then all $\{1, x, x^2, \dots, x^{d-1}\}$ (distinct)

satisfy the congruence $y^d \equiv 1\ (p)$.

By FACT (☆) they're all the solutions!

Thus any $b \in \mathbb{Z}_p^\times$ of order d is of the form

$b = x^i$ some $0 \le i < d$. Now, the "order-formula"

$$d = \mathrm{ord}(b) = \mathrm{ord}(x^i) = \frac{\mathrm{ord}(x)}{GCD(i, \mathrm{ord}(x))} = \frac{d}{GCD(i,d)}$$

shows $GCD(i,d) = 1$.

Conclude: $N_d = \#\{i : x^i \text{ has order } d\} = \varphi(d)$.

$\Rightarrow$ CLAIM ✓

Finally, since we have the ϕ — sum formula

$$\sum_{d \mid p-1} \phi(d) = p-1$$

no N_d can be 0. Thus $N_d = \phi(d)$, $\forall d \mid p-1$.

$d = p-1$: $\mathbb{Z}_p^\times$ has $\phi(p-1)$ elements of order $p-1$

i.e., generators. $\square$