Lecture 17 Friday Feb 26

For $a \in \mathbb{Z}_N^\times$ let

$\langle a \rangle$ = subgroup of $\mathbb{Z}_N^\times$ generated by a

LEM 9 For $N = 2^n$, $n \geq 3$

In the group $\mathbb{Z}_N^\times$ the subgroup

$\langle 3 \rangle$ has order $N/4$

pf the order divides $|\mathbb{Z}_N^\times| = 2^{n-1}$ by Lagrange

So order $= 2^r$ $1 \leq r \leq n-1$

Show $r = n-2$.

For $1 \leq l$,

$$3^{2^l} - 1 = 2^{l+2} \theta_l$$ by L2.

Take $l = r$

$$0 \equiv 3^{2^r} - 1 \equiv 2^{r+2} \theta_r \pmod N$$

(θ_r: unit in $\mathbb{Z}_N$)

So $0 \equiv 2^{r+2}$

$N \mid 2^{r+2}$

$r \geq n-2$

Now take $l = n-2$

$$3^{2^{n-2}} - 1 \equiv 2^n \theta_{n-2} \pmod N$$

($2^n = N$)

$\equiv 0$ So $r \leq n-2$ $\square$

LEM 10 For $N = 2^n$, $n \geq 3$

In the group $\mathbb{Z}_N^\times$,

$$-1 \notin \langle 3 \rangle$$

pf Suppose

$$-1 \in \langle 3 \rangle$$

$\exists$ integer $a \geq 1$ s.t.

$$3^a \equiv -1 \pmod{N}$$

Suppose a is even

$$a = 2b$$

$$-1 \equiv 3^{2b} \equiv (3^b)^2 \pmod{N}$$

Contradicts LEM 7 (ii)

So a is odd

obs $(-3)^a = 1$

Let q = order of $\langle -3 \rangle$

$q \mid a$ so q is odd.

$q \neq 1$ since $-3 \neq 1 \pmod{N}$

Also $q \mid |\mathbb{Z}_N^\times| = 2^{n-1}$ by Lagrange

q even cntr.

□

Prop 11 For $N = 2^n$, $n \geq 3$

$\exists$ group isomorphism

$$\varphi : \quad \mathbb{Z}_{N/4} \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_N^\times$$

that sends

$$\left(a + \tfrac{N}{4}\mathbb{Z},\ b + 2\mathbb{Z}\right) \longrightarrow 3^a(-1)^b \qquad *$$

$\forall$ all $a, b \in \mathbb{Z}$.

pf By LEM 8 and since $(-1)^2 = 1$ $\exists$ group hom φ that satisfies *.

φ is injective by LEM 10

φ is a bijection since

$$|\mathbb{Z}_{N/4} \times \mathbb{Z}_2| = |\mathbb{Z}_N^\times|$$

$$\| \qquad\qquad \| \qquad\qquad \| N/2$$

$$|\mathbb{Z}_{N/4}|\ |\mathbb{Z}_2|$$

$$\| \qquad \| 2$$

$$N/4$$

□

Find $Z_N^\times$ for $N = p^n$, odd prime p, $n \geq 2$

Ex 12 $N = 3^2 = 9$

Z_9 : $\not{0}$ 1 2 $\not{3}$ 4 5 $\not{6}$ 7 8

$Z_9^\times$: 1 2 4 5 7 8

$4 = 2^2$, $5 = 2^5$, $7 = 2^4$, $8 = 2^3$

$2^6 = 1$

2 generates $Z_9^\times$

$Z_9^\times$ is cyclic.

— ∘ —

We will show that $Z_N^\times$ is cyclic always

Since $N = p^n$

$$|\mathbb{Z}_N^\times| = p^n - p^{n-1} = (p-1)p^{n-1}$$

↑ ↑
not prime

Apply LEM 1 to $\mathbb{Z}_N^\times$

Define

$$A = \{ a \in \mathbb{Z}_N^\times \mid a^{p-1} = 1 \}$$

$$B = \{ b \in \mathbb{Z}_N^\times \mid b^{p^{n-1}} = 1 \}$$

So $|A| = p-1$, $|B| = p^{n-1}$

Also the map

$$A \times B \longrightarrow \mathbb{Z}_N^\times$$

$$(a, b) \longrightarrow ab$$

is an iso of grps

We show A, B are both cyclic.

LEM 13 The group A is cyclic.

pf Consider the ring homomorphism

$$\begin{aligned} \mathbb{Z}_N &\longrightarrow \mathbb{Z}_p \qquad * \\ r + N\mathbb{Z} &\longrightarrow r + p\mathbb{Z} \end{aligned}$$

$*$ is surj

$*$ induces surj group hom

$$\varphi: \quad \mathbb{Z}_N^{\times} \longrightarrow \mathbb{Z}_p^{\times}$$

show $\ker(\varphi) = B$

Since φ is surj

$$|\ker(\varphi)| = |\mathbb{Z}_N^{\times}| / |\mathbb{Z}_p^{\times}| = p^{n-1} = |B|$$

show $B \subseteq \ker(\varphi)$:

$\forall b \in B$

$$b^{p^{n-1}} = 1$$

So

$$\varphi(b)^{p^{n-1}} = 1$$

So $\varphi(b)$ has order a power of p

By Lagrange, order of $\varphi(b)$ divides $|\mathbb{Z}_p^{\times}| = p-1$

So $\varphi(b)$ has order 1 ie $\varphi(b) = 1$

So $\ker(\varphi) = B$

Now the restriction of φ to A induces a group iso

$$\varphi/_A : A \to \mathbb{Z}_p^\times$$

Recall $\mathbb{Z}_p^\times$ is cyclic so A is cyclic. $\square$

Next we show that B is cyclic.

We use a result about our odd prime p

LEM 14 Fix $x \in \mathbb{Z}$ and $t = 1, 2, \ldots$

TFAE:

(i) $x \equiv 1 \pmod{p^t}$

(ii) $x^p \equiv 1 \pmod{p^{t+1}}$

pf (i) $\rightarrow$ (ii) Write

$$x = 1 + a p^t \qquad a \in \mathbb{Z}$$

So

$$x^p = (1 + a p^t)^p$$

$$= \sum_{k=0}^{p} \binom{p}{k} a^k p^{tk}$$ Binom thm

$$= 1 + p a p^t + \sum_{k=2}^{p} \binom{p}{k} a^k p^{tk}$$

p^{t+1} divides

$$\equiv 1 \pmod{p^{t+1}}$$

(ii) → (i) Use induction on t

Case $t=1$ Given

$$x^p \equiv 1 \pmod{p^2}$$

So $$x^p \equiv 1 \pmod{p}$$

Also since $|\mathbb{Z}_p^\times| = p-1$,

$$x^{p-1} \equiv 1 \pmod{p}$$ by Cauchy thm

So $$x \equiv 1 \cdot x \equiv x^{p-1}x \equiv x^p \equiv 1 \pmod{p}$$

Case $t \geq 2$ Given

$$x^p \equiv 1 \pmod{p^{t+1}}$$

So $$x^p \equiv 1 \pmod{p^t}$$

By induction

$$x \equiv 1 \pmod{p^{t-1}}$$

Write

$$x = 1 + b\,p^{t-1} \qquad b \in \mathbb{Z}$$

show $p \mid b$

obs

$$x^p = \left(1 + b\,p^{t-1}\right)^p$$

$$= \sum_{k=0}^{p} \binom{p}{k} b^k\, p^{k(t-1)}$$

$$= 1 + p\,b\,p^{t-1} + \underbrace{\binom{p}{2} b^2\, p^{2t-2}}_{p^{\frac{p-1}{2}}} + \sum_{k=3}^{p} \binom{p}{k} b^k\, p^{k(t-1)}$$

$$\binom{p}{2} b^2\, p^{2t-2} = \frac{p-1}{2}\, b^2\, p^{2t-2}$$

$[2t-1 \geq t+1]$

$[k(t-1) \geq t+1]$

p^{t+1} divides

So

$$x^p \equiv 1 + b\,p^t \pmod{p^{t+1}}$$

$$\| \quad 1$$

So $\quad 0 \equiv b\,p^t \pmod{p^{t+1}}$

so $\quad p \mid b$

□

2/26/16

COR 15 In the group $\mathbb{Z}_N^\times$ the equation

$$x^p = 1$$

has exactly p solutions

$$1,\ 1+p^{n-1},\ 1+2p^{n-1},\ \ldots,\ 1+(p-1)p^{n-1}$$

pf Set $t = n-1$ in LEM 14 and recall $N = p^n$ □