Lecture 16 Wednesday Feb 24

Given a field F

Consider polynomial ring $F[x]$

Given $0 \neq f \in F[x]$

LEM 3

$$|\{a \in F \mid f(a) = 0\}| \leq \deg(f)$$

pf $F[x]$ is a UFD

Factor f into a product of irreducibles

$$f = f_1 f_2 \cdots f_t$$

$$\deg(f) = \sum_{i=1}^{t} \deg(f_i) \geq t$$

$\deg(f_i) \geq 1$

$\forall a \in F$

$f(a) = 0$ implies $x - a$ among f_i

Result follows $\square$

Prop 4 Given a field F

Let G denote a finite subgroup of $F^\times$

Then G is cyclic.

pf We invoke LEM 2

For each positive integer d that divides $|G|$,

show

$$|\{a \in G \mid a^d = 1\}| \leq d$$

Consider the polynomial ring

$$F[x]$$

Consider polynomial

$$f(x) = x^d - 1$$

Obs

$$|\{a \in G \mid a^d = 1\}| \leq |\{a \in F \mid f(a) = 0\}| \leq \deg(f) = d$$

LEM 3

Result follows by LEM 2. □

COR 5 For a finite field F

the group of units $F^\times$ is cyclic.

Ex 6 For a positive integer prime p

recall the ring

$$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$$

is a field. The group $\mathbb{Z}_p^\times$ is cyclic

by Cor 5.

Next goal

Given integer $N \geq 2$

Recall ring

$$\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$$

View

$$\mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\}$$ $+, \times$ computed modulo N

Find the group of units

$$\mathbb{Z}_N^{\times}$$

Earlier we reduced the problem to the case

$$N = p^n \qquad p \text{ prime}, \qquad n = 1, 2, \ldots$$

Here

$$\left|\mathbb{Z}_N^{\times}\right| = p^n - p^{n-1}$$

Now consider subcases $p = 2$, p odd.

Find $\mathbb{Z}_N^\times$ for $N = 2^n$, $n \geq 1$.

Obs

$$\mathbb{Z}_N^\times = \{ 1, 3, 5, \ldots, N-1 \}$$

$$|\mathbb{Z}_N^\times| = 2^{n-1} = N/2$$

Examples

n	N	Describe $\mathbb{Z}_N^\times$	$\mathbb{Z}_N^\times$ is iso to
1	2	1	1
2	4	$1, 3 \; (=-1)$ $\quad (-1)^2 = 1$	$\mathbb{Z}_2$
3	8	$1, 3, 5 \; (=-3), 7 \; (=-1)$ $\quad 3^2 = 9 \equiv 1$ $\quad (-3)^2 = 9 \equiv 1$ $\quad (-1)^2 = 1$ each non identity element has order 2	$\mathbb{Z}_2 \times \mathbb{Z}_2$

For $n \geq 3$ we will display a group iso

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

LEM 7 For $N = 2^n$, $n \geq 3$

In $Z_N^\times$:

(i) $x^2 = 1$ has exactly 4 sols

$x = 1, \quad x = -1, \quad x = \frac{N}{2} + 1, \quad x = \frac{N}{2} - 1$ *

(ii) $x^2 = -1$ has no solutions.

pf (i) Obs * are sols:

$$\left(\frac{N}{2} \pm 1\right)^2 = \frac{N^2}{4} \pm 2\frac{N}{2} + 1$$

$$= \frac{N}{4} N \pm N + 1$$

$\equiv 0 \pmod N$ $\equiv 0 \pmod N$

show * are only sols

Given odd $x \in Z$ s.t.

$x^2 \equiv 1 \pmod N$, $\quad x \not\equiv \pm 1 \pmod N$

show

$$x \equiv \frac{N}{2} \pm 1 \pmod N$$

Obs

$$0 \equiv x^2 - 1 \equiv (x-1)(x+1) \pmod N$$

↑ ↑

even

2/24/16
*

Write

$$x-1 = 2^r a \qquad \text{odd } a \in \mathbb{Z}, \qquad 1 \le r \le n-1$$

$$x+1 = 2^s b \qquad \text{odd } b \in \mathbb{Z}, \qquad 1 \le s \le n-1$$

So

$$0 \equiv (x-1)(x+1) \equiv 2^{r+s}\, ab \pmod{N}$$

So

N divides $2^{r+s}\, ab$

$N = 2^n$; ab odd

So

$$n \le r+s$$

Show $r=1$ or $s=1$

Suppose not. So

$r \ge 2$, $s \ge 2$

$4 \mid x-1$, $4 \mid x+1$

4 divides $x-1 + x+1 = 2x$ ↑ weird

cont.

So either

$r = n-1$ and $s = 1$ ☆

or

$r = 1$ and $s = n-1$ ☆☆

For ✡

$$x-1 = 2^{n-1} a \qquad a \text{ odd}$$

write

$$a = 1 + 2k \qquad k \in \mathbb{Z}$$

So mod N,

$$x \equiv 1 + 2^{n-1} a$$

$$\equiv 1 + 2^{n-1}(1 + 2k)$$

$$\equiv 1 + \underbrace{2^{n-1}}_{\| \; N/2} + \underbrace{2^{n}}_{\| \; N \; \| \; 0} k$$

$$\equiv N/2 + 1$$

Similarly in case ✡✡,

$$x \equiv \frac{N}{2} - 1 \pmod{N}$$

(ii) Suppose $\exists \quad x \in \mathbb{Z} \quad$ st

$$x^2 \equiv -1 \pmod{N}$$

$N \quad / \quad x^2+1$

N
$\|$
$2^\wedge$

$4 \mid N$

$4 \mid x^2+1$

we saw earlier this cannot occur. cntr. □

Consider

$$3-1, \quad 3^2-1, \quad 3^4-1, \quad 3^8-1, \quad 3^{16}-1, \ \ldots$$

Express as power of 2 times an odd integer

$$3-1 = 2 \cdot 1$$

$$3^2-1 = 2^3 \cdot 1$$

$$3^4-1 = 2^4 \cdot 5$$

$$3^8-1 = 2^5 \cdot 205$$

$$\ldots$$

LEM 8 For each integer $\ell \geq 1$, $\exists$ odd integer θ_ℓ

st $$3^{(2^\ell)} - 1 = 2^{\ell+2}\theta_\ell$$

pf By induction on $\ell = 1, 2, \ldots$

$\ell = 1$ $\quad \theta_\ell = 1$ ✓

Assume $\ell \geq 2$ We have

$$3^{2^\ell} = 3^{2^{\ell-1} 2}$$

$$= \left(3^{2^{\ell-1}}\right)^2$$

$$= \left(2^{\ell+1}\theta_{\ell-1} + 1\right)^2 \quad \text{by ind}$$

$$= 2^{2\ell+2}\theta_{\ell-1}^2 + 2^{\ell+2}\theta_{\ell-1} + 1$$

2/27/16

$$= 2^{l+2}\theta_{l-1}\underbrace{\left(\underbrace{2^{l}\theta_{l-1}}_{\text{even}} + \underbrace{1}_{\text{odd}}\right)}_{\text{odd}} + 1$$

$$= \theta_l \text{ odd}$$

So

$$3^{2^l} - 1 = 2^{l+2}\theta_l \qquad \theta_l \text{ odd}$$

□

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

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

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

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 $r = n-2$.

Fix $1 \leq l$,

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

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 $l = n-2$

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

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