Lecture 10 Wednesday Feb 10

claim $\exists\ a \in \mathbb{Z}_p^{\times}$ s.t.

$$a^{\frac{p-1}{2}} = -1 \qquad *$$

pf of claim Suppose not. Then $\forall a \in \mathbb{Z}_p^{\times}$,

$$a^{\frac{p-1}{2}} = 1$$

Consider polynomial

$$f(\lambda) = \lambda^{\frac{p-1}{2}} - 1 \qquad \in \mathbb{Z}_p[\lambda]$$

$$f(a) = a^{\frac{p-1}{2}} - 1 = 0$$

In $\mathbb{Z}_p[\lambda]$, divide $f(\lambda)$ by $\lambda - a$ and consider the remainder r:

$$f(\lambda) = (\lambda - a)\, q(\lambda) + r$$

$q(\lambda) \in \mathbb{Z}_p[\lambda]$, $r \in \mathbb{Z}_p$

Set $\lambda = a$:

$$0 = \underbrace{(a-a)}_{=0}\, g(a) + r$$

$$r = 0$$

$\lambda - a$ divides $f(\lambda)$ $\quad \forall\, a \in \mathbb{Z}_p^{\times}$

So $\prod_{a \in \mathbb{Z}_p^{\times}} (\lambda - a)$ divides $f(\lambda)$

degree: $p-1$ $\qquad \frac{p-1}{2}$

Impossible

claim proved ✓

Note $\frac{p-1}{4} \in \mathbb{Z}$

Define $y \in \mathbb{Z}_p^{\times}$ by

$$y = a^{\frac{p-1}{4}}, \qquad a \text{ from } *$$

So

$$y^2 = a^{\frac{p-1}{2}} = -1$$

Recall canonical ring hom

$$\varphi: \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}_p \\ r & \longrightarrow & r + p\mathbb{Z} \end{array}$$

is surjective with kernel $p\mathbb{Z}$

$\exists \; x \in \mathbb{Z} \quad st \quad \varphi(x) = y$

Obs

$$\varphi(x^2+1) = y^2+1 = 0$$

So

$$x^2+1 \in p\mathbb{Z}$$

So

$$x^2+1 \equiv 0 \pmod{p}$$

□

LEM 14 Given a prime integer $p \geq 2$ such that

$$p \not\equiv 3 \pmod 4$$

then $\exists\ a, b \in \mathbb{Z}$ such that

$$p = a^2 + b^2$$

pf For $p = 2$ take $a = 1,\ b = 1$

$$2 = 1^2 + 1^2 \quad \checkmark$$

Now assume p is odd. So

$$p \equiv 1 \pmod 4$$

In $\mathbb{Z}[i]$ write p as a product of primes:

$$p = p_1 p_2 \cdots p_n \qquad n \geq 1$$

Apply norm:

$$p^2 = N(p) = N(p_1)\, N(p_2) \cdots N(p_n)$$

$\uparrow \quad \uparrow \quad \cdots \quad \uparrow$

integers ≥ 2

Either

(i) $n=1$, ie p is prime in $\mathbb{Z}[i]$

or

(ii) $n=2$ and $N(p_1) = p$, $N(p_2) = p$

Suppose (i). By LEM 13 $\exists\ x \in \mathbb{Z}$ st

$$x^2+1 \equiv 0 \pmod{p}$$

So

$$p \mid x^2+1$$

In $\mathbb{Z}[i]$,

$$x^2+1 = (x+i)(x-i)$$

In $\mathbb{Z}[i]$,

$$p \mid x+i \quad \text{or} \quad p \mid x-i$$

So $\exists\ \alpha+\beta i \in \mathbb{Z}[i]$ st

$$p(\alpha+\beta i) = x+i \quad \text{or} \quad p(\alpha+\beta i) = x-i$$

Get

$$p\alpha = x \quad \text{and} \quad p\beta = \mp 1$$

↑

p is unit in $\mathbb{Z}$, cont

So (i) cannot occur

So (ii) holds

$p = p_1 p_2$ $\qquad N(p_1) = p = N(p_2)$

write $p_1 = a + bi$ $\qquad a, b \in \mathbb{Z}$

so

$p = N(p_1) = a^2 + b^2$ □

LEM 15 For an integer $x \geq 1$ TFAE

(i) x is prime in $\mathbb{Z}[i]$

(ii) x is prime in $\mathbb{Z}$ and

$x \equiv 3 \pmod 4$

pf (i) → (ii) x is prime in $\mathbb{Z}$ ✓

shw $x \equiv 3 \pmod 4$

$x \neq 2$ since $2 = (1+i)(1-i)$ is not prime in $\mathbb{Z}[i]$

So x is odd

$x \equiv 1 \pmod 4$ or $x \equiv 3 \pmod 4$

Suppose $x \equiv 1 \pmod 4$

By LEM 14 $\exists\ a, b \in \mathbb{Z}$ st

$$x = a^2 + b^2$$

Then in $\mathbb{Z}[i]$,

$$x = (a+bi)(a-bi)$$

$a+bi$, $a-bi$ not units since $a^2+b^2 = x \neq 1$

So x not prime in $\mathbb{Z}[i]$ cont.

So

$$x \equiv 3 \pmod 4$$

(ii) → (i) Suppose x not prime in $\mathbb{Z}[i]$

Write $x = yz$ nonunits $y, z \in \mathbb{Z}[i]$

Take norm:

$$x^2 = N(x) = N(y)\,N(z)$$

↑ ↑ integers ≥ 2

Get $N(y) = x$, $N(z) = x$

Write $y = a + bi$ $a, b \in \mathbb{Z}$

$$x = N(y) = a^2 + b^2$$

Mod 4,

$$3 \equiv x \equiv a^2 + b^2 \not\equiv 3$$

$a^2 + b^2 \bmod 4$: cases

a \ b	0	1	2	3
0	0	1	0	1
1	1	2	1	2
2	0	1	0	1
3	1	2	1	2

Conc. So x is prime in $\mathbb{Z}[i]$.

□

LEM 16 For nmo integers a, b TFAE:

(i) $a+bi$ is prime in $\mathbb{Z}[i]$

(ii) a^2+b^2 is prime in $\mathbb{Z}$

pf (i) $\to$ (ii) Suppose not.

Write $a^2+b^2 = rs$ nm units $r, s \in \mathbb{Z}$

$$= (a+bi)(a-bi)$$

↑ ↗ primes

WLOG $r = (a+bi)u$ unit $u \in \mathbb{Z}[i]$

$s = (a-bi)\bar{u}$

Imposs since $a, b, r, s \in \mathbb{Z}$ $a \neq 0, b \neq 0$

$u \in \{\pm 1, \pm i\}$

$(i) \to (i)$ Suppose not

write

$$a+bi = xy$$

nonunits $x, y \in \mathbb{Z}[i]$

Apply norm

$$a^2+b^2 = N(x)N(y)$$

↑ prime integer

↑ ↑ integers ≥ 2

cont

□

Thm 17 The primes in $\mathbb{Z}[i]$ are:

(i) $\pm p, \pm ip$ p prime in $\mathbb{Z}$, $p \equiv 3 \pmod 4$

(ii) $a+bi$ $a, b \in \mathbb{Z}$ a^2+b^2 prime in $\mathbb{Z}$

pf By LEM 15, 16. □