Last time: $p \in \mathbb{Z}$ a (non-zero) prime

p factors in $\mathbb{Z}(i)$ $\longleftrightarrow$ x^2+1 factors in $\mathbb{Z}_p[x]$

example: $p = 97 = 81 + 16 = 9^2 + 4^2 = (9+4i)(9-4i)$

in $\mathbb{Z}_{97}[x]$, $x^2+1 = (x-22)(x+22)$

connection? in $\mathbb{Z}_{97}$, $4/9 = 22$, $9/4 = -22$

=

input from ring theory:

$$\mathbb{Z}[i]/\langle p \rangle \cong \mathbb{Z}_p[x]/\langle x^2+1 \rangle$$

$$\overline{a+bi} \longleftrightarrow \overline{\bar{a}+\bar{b}x}$$

because both $\cong \mathbb{Z}[x]/\langle x^2+1, p \rangle$

$$\mathbb{Z}[x] \longrightarrow \mathbb{Z}[i] \longrightarrow \mathbb{Z}[i]/\langle p \rangle$$

$f = a+bx+cx^2+\cdots \longmapsto f(i) = a+bi+ci^2+\cdots$

$a+bi \longmapsto \overline{a+bi}$

$\mathbb{Z}_p[x]$ $\quad \bar{f} = \bar{a}+\bar{b}x+\bar{c}x^2+\cdots$

$\mathbb{Z}_p[x]/\langle x^2+1 \rangle$ $\quad \bar{g}$

both ways, get a surj. ring hom. with ker $= \langle p, x^2+1 \rangle$

use 1st iso thm

kernel of $\to$?

take $f \in \mathbb{Z}[x]$

then $\bar{f} = 0$ in $\mathbb{Z}_p[x]/\langle x^2+1\rangle$

so $\bar{f} = (x^2+1)\cdot \bar{g}$ for some $\bar{g} \in \mathbb{Z}_p[x]$ or $g \in \mathbb{Z}[x]$

so $\bar{f} - (x^2+1)\bar{g}$ is 0 in $\mathbb{Z}_p[x]$

so $f - (x^2+1)g$ is a mult. of p in $\mathbb{Z}[x]$

so $f - (x^2+1)g = 3h$ for some $h \in \mathbb{Z}[x]$

so $f = (x^2+1)g + 3h$ so $f \in \langle x^2+1, 3\rangle$

(may help on HW 5 last problem?)

Worksheet:

$$\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[x]/\langle x^2+5\rangle$$

$$a+b\sqrt{-5} \longleftrightarrow a+bx$$

$$3 \longleftrightarrow 3$$

$$1+\sqrt{-5} \longleftrightarrow 1+x$$

$$\mathbb{Z}[\sqrt{-5}]/\langle 3, 1+\sqrt{-5}\rangle \cong \mathbb{Z}[x]/\langle x^2+5, 3, 1+x\rangle$$

$$\cong$$

$$\mathbb{Z}_3[x]/\langle x^2+5, x+1\rangle$$

as subsets of $\mathbb{Z}_3[x]$, $\langle x^2+5, x+1\rangle = \langle x+1\rangle$ are the same set.

$x^2+5 = (x+1)(x+2)$ in $\mathbb{Z}_3[x]$ $\quad x^2+5 \in \langle x+1\rangle$

$$\mathbb{Z}_3[x]/\langle x+1\rangle \cong \mathbb{Z}_3$$

Challenge problem: $\mathbb{Z}[\sqrt{-5}]/\langle 1+\sqrt{-5}\rangle \cong \mathbb{Z}[x]/\langle x^2+5,\ x+1\rangle$

one way to think: as subsets of $\mathbb{Z}[x]$,

$$\langle x^2+5,\ x+1\rangle = \langle x+1,\ 6\rangle$$

$$\begin{array}{r} x-1 \\ x+1 \overline{)\ x^2+5} \\ \vdots \\ 6 \end{array}$$

$$x^2+5 = (x+1)(x-1)+6$$

$$6 = (x^2+5) - (x+1)(x-1)$$

and then $\mathbb{Z}[x]/\langle 6,\ x+1\rangle = \mathbb{Z}_6[x]/\langle x+1\rangle = \mathbb{Z}_6$

another way: $\mathbb{Z}[x]/\langle x+1\rangle \cong \mathbb{Z}$

$$\bar{f} \longleftrightarrow f(-1)$$

$$x^2+5 \longleftrightarrow 6$$

$$\mathbb{Z}[x]/\langle x+1,\ x^2+5\rangle \cong \mathbb{Z}/\langle 6\rangle$$

fun exercise: think about $\mathbb{Z}[i]/\langle 2+i\rangle \cong \mathbb{Z}_5$ in these terms.

Last problem of HW5: $a, b \in R$

$$R/_{\langle a,b\rangle} \cong R/_{\langle a\rangle}\Big/_{\langle \bar{b}\rangle}$$

or $R/_{\langle b\rangle}\Big/_{\langle \bar{a}\rangle}$

after the break:

$$\mathbb{Z}[\sqrt{-5}]/_{\langle 2,\, 1+\sqrt{-5}\rangle} \cong \mathbb{Z}[\sqrt{-5}]/_{\langle 2\rangle}\Big/_{\langle \overline{1+\sqrt{-5}}\rangle}$$

$$\cong \mathbb{Z}[\sqrt{-5}]/_{\langle 1+\sqrt{-5}\rangle}\Big/_{\langle \bar{2}\rangle}$$

Very last thing about rings.

Classify all rings with 4 elements up to iso.
what could it look like?

- have 0.
- have $1 \neq 0$.
- have $2 = 1+1$.
  - maybe $2 \neq 0$ $\rightsquigarrow \mathbb{Z}_4$
  - maybe $2 = 0$
    - $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_2[x]/_{\langle x^2+x\rangle}$
    - $\mathbb{Z}_2[x]/_{\langle x^2\rangle} \cong \mathbb{Z}_2[x]/_{\langle x^2+1\rangle}$
    - $\mathbb{Z}_2[x]/_{\langle x^2+x+1\rangle}$ (field with 4 elts.)

first: if $2 \neq 0$.

let $3 = 2 + 1$

can't have $3 = 2$, otherwise $1 = 0$

can't have $3 = 1$, otherwise $2 = 0$

can we have $3 = 0$? No

↳ if so, let x be the 4th elt. of our ring.

$x+1$ must be one of the 4 that we already have.

if $x+1 = 0$ then $x = 2$ (nope)

if $x+1 = 1$ then $x = 0$ (nope)

if $x+1 = 2$ then $x = 1$ (nope)

if $x+1 = x$ then $1 = 0$ (nope)

. so 3 is a new element.

$R = \{0, 1, \underbrace{2}_{=1+1}, \underbrace{3}_{=1+1+1}\} \cong \mathbb{Z}_4$

second: if $2 = 0$

take another element, call it x.

then $x+1 \neq 0$ bec. $x \neq 1$

$x+1 \neq 1$ bec. $x \neq 0$

$x+1 \neq x$ bec. $1 \neq 0$

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

so $R = \{0, 1, x, x+1\}$

$x + x = x(1+1) = x \cdot 0 = 0$

$x^2 = ?$

then $x \cdot (x+1) = x^2 + x = ? + x$

and $(x+1)^2 = x^2 + 1 = ? + 1$

x	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	?	? + x
x+1	0	x+1	? + x	? + 1

$\mathbb{Z}[\sqrt{-5}]/2$

if $x^2 = 0$, our ring is $\mathbb{Z}_2[x]/\langle x^2 \rangle$

if $x^2 = 1$, then $x^2 + 1 = 0$ and we've got $\mathbb{Z}_2[x]/\langle x^2+1 \rangle$

if $x^2 = x$, then $x^2 + x = 0$, and it's $\mathbb{Z}_2(x)/\langle x^2+x \rangle$

$\cong \mathbb{Z}_2 \times \mathbb{Z}_2$

if $x^2 = x+1$ then $x^2 + x + 1 = 0$ and

we've got $\mathbb{Z}_2[x]/\langle x^2+x+1 \rangle$

(field with 4 elements)