Theorem (Fermat):
a prime number p can be written as a^2+b^2 iff $p=2$ or $p \equiv 1 \pmod 4$

Outline of the proof:

first, these are equivalent:

1. $p = a^2+b^2$
2. p factors in $\mathbb{Z}[i]$
3. $\mathbb{Z}[i]/\langle p \rangle$ is not an integral domain
4. $\mathbb{Z}[x]/\langle x^2+1, p \rangle$ is not an integral domain
5. $\mathbb{Z}_p[x]/\langle x^2+1 \rangle$ is not an integral domain
6. x^2+1 factors in $\mathbb{Z}_p[x]$
7. x^2+1 has a root in $\mathbb{Z}_p$

then: (1) $\Rightarrow$ $p=2$ or $p \equiv 1 \pmod 4$ (saw this last week)

$p=2$ or $p \equiv 1 \pmod 4$ $\Rightarrow$ (7) (worksheet Monday...) ☆

(1) $\Leftrightarrow$ (2) saw it last week

(6) $\Leftrightarrow$ (7) saw it last term.

(5) $\Leftrightarrow$ (6) saw it last Friday.

(2) $\Leftrightarrow$ (3) is similar bec. $\mathbb{Z}[i]$ has a div. alg.

(3) $\Leftrightarrow$ (4) $\Leftrightarrow$ (5) because those 3 rings are isomorphic ☆

Prop if $p = 2$ or $p \equiv 1 \pmod 4$ then $x^2 + 1$ has a root in $\mathbb{Z}_p$.

Proof for $p = 2$, take $x = 1$

otherwise, write $p = 4k+1$, and let $x = \bar{1} \cdot \bar{2} \cdot \cdots \cdot \overline{2k} \in \mathbb{Z}_p$

then $x = (-\bar{1})(-\bar{2}) \cdots (-\overline{2k})$ because even # of -1s

$= \overline{4k} \cdot (\overline{4k-1}) \cdots (\overline{2k+1})$ bec. we're in $\mathbb{Z}_{4k+1}$

now $x^2 = \bar{1} \cdot \bar{2} \cdot \bar{3} \cdot \cdots \cdot \overline{4k}$ product of everything in $\mathbb{Z}_p$ other than 0.

I claim that this $= -\bar{1}$

bec. we have $\bar{1}$ and $-\bar{1}$, and everything else comes in pairs $a \cdot a^{-1}$

p is a prime, so every non-zero $a \in \mathbb{Z}_p$ has a multiplicative inverse, and $(a^{-1})^{-1} = a$ so they come in pairs,

unless $a = a^{-1}$

equivalently, $a^2 = 1$

$a^2 - 1 = 0$

$(a+1)(a-1) = 0$

$a + 1 = 0$ or $a - 1 = 0$

$a = 1$ or $a = -1$

because $\mathbb{Z}_p[a]$ is an int. dom! / could fail for $p = 21$?

so $x^2 = \bar{1} \cdot \cancel{\bar{2}} \cdot \cancel{\bar{3}} \cdot \cancel{X} \cdot \cancel{X} \cdot \overline{4k} = -\bar{1}$

so $x^2 + \bar{1} = 0$

□

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

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

$\overline{2+3i} \longleftrightarrow \overline{\bar{2}+\bar{3}x}$

idea: $\mathbb{Z}_p[x]/\langle x^2+1\rangle$ = take polynomials in $\mathbb{Z}_p[x]$ and declare $x^2+1=0$ see where it takes you

$\mathbb{Z}[i]/\langle p\rangle$ = take $\mathbb{Z}[i]$, force $p=0$, see where that takes you.

$\mathbb{Z}[x]/\langle x^2+1,\ p\rangle$ kill both x^2+1 and p at the same time,

or kill x^2+1 first to get $\mathbb{Z}[i]$ and then kill 3

or kill 3 to get $\mathbb{Z}_3[x]$ and then kill x^2+1

remember: $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$ because of

$\varphi: \mathbb{R}[x] \longrightarrow \mathbb{C}$

$f \longmapsto f(i)$

$f(i)=0 \Rightarrow f(-i)=0$, so

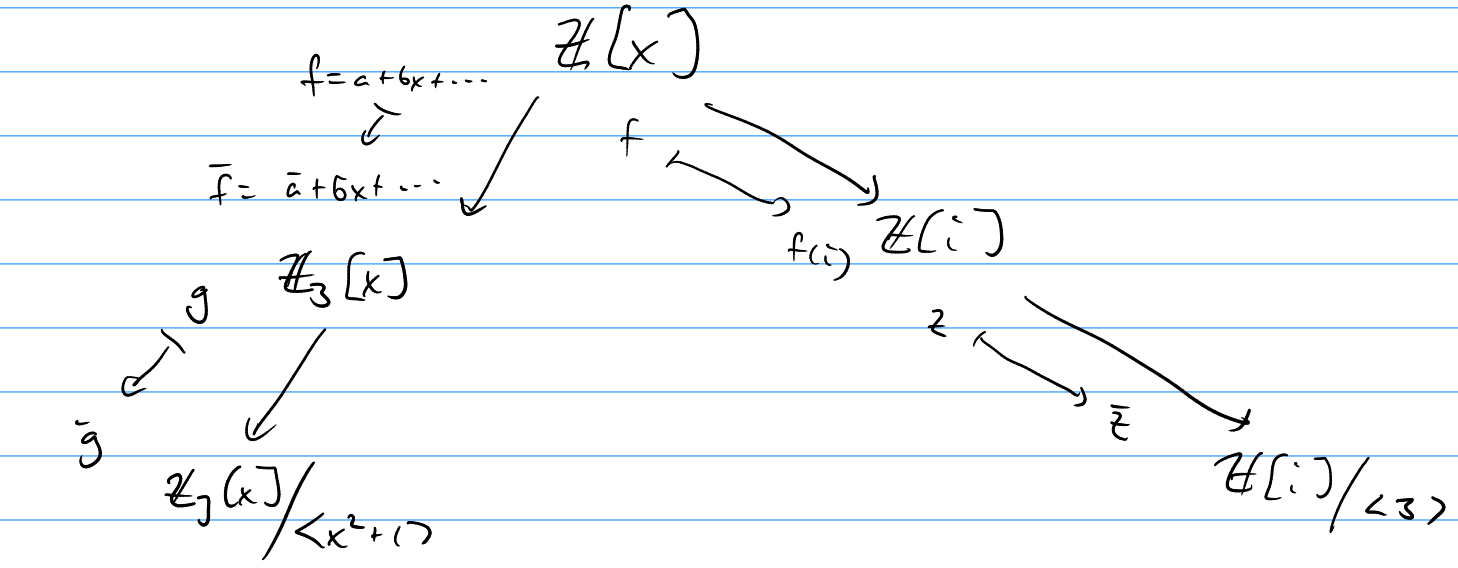
$x-i$ and $x+i$ both divide f $\qquad \ker\varphi = \langle x^2+1\rangle$

Similarly, the map $\mathbb{Z}[x] \longrightarrow \mathbb{C}$
$f \longmapsto f(i)$

image is $\mathbb{Z}[i] \subset \mathbb{C}$
kernel is $\langle x^2+1 \rangle \subset \mathbb{Z}[x]$
1st iso thm gives $\mathbb{Z}[i] \cong \mathbb{Z}[x]/\langle x^2+1 \rangle$.

upcoming homework: $R/\langle a,b \rangle \cong \left(R/\langle a \rangle\right)/\langle \bar{b} \rangle$

$\cong \left(R/\langle b \rangle\right)/\langle \bar{a} \rangle$



claim: kernel is $\langle 3, x^2+1 \rangle$
either way.

if $f \in \mathbb{Z}[x]$ satisfies $\overline{f(i)} = \bar{0}$ in $\mathbb{Z}[i]/\langle 3 \rangle$

then $f(i) = 3 \cdot (a+bi)$
so $f(i) - 3(a+bi) = 0$
so $f(x) - 3(a+bx) = (x^2+1) \cdot g$
so $f = 3(a+bx) + (x^2+1)g$ so $f \in \langle 3, x^2+1 \rangle$