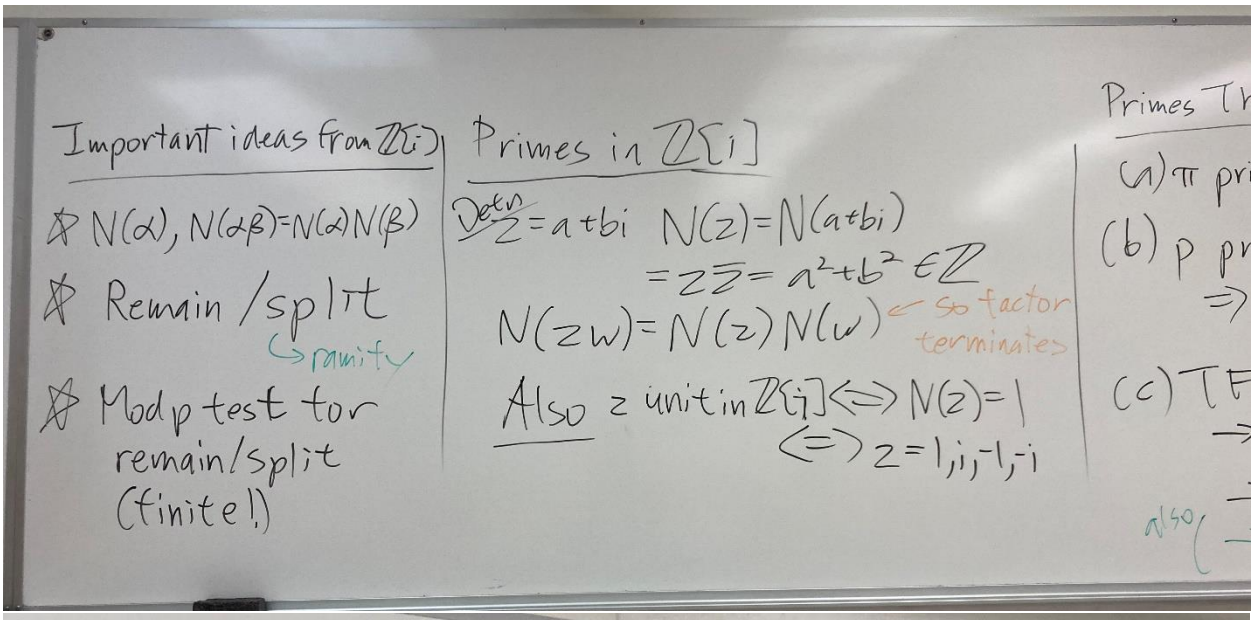
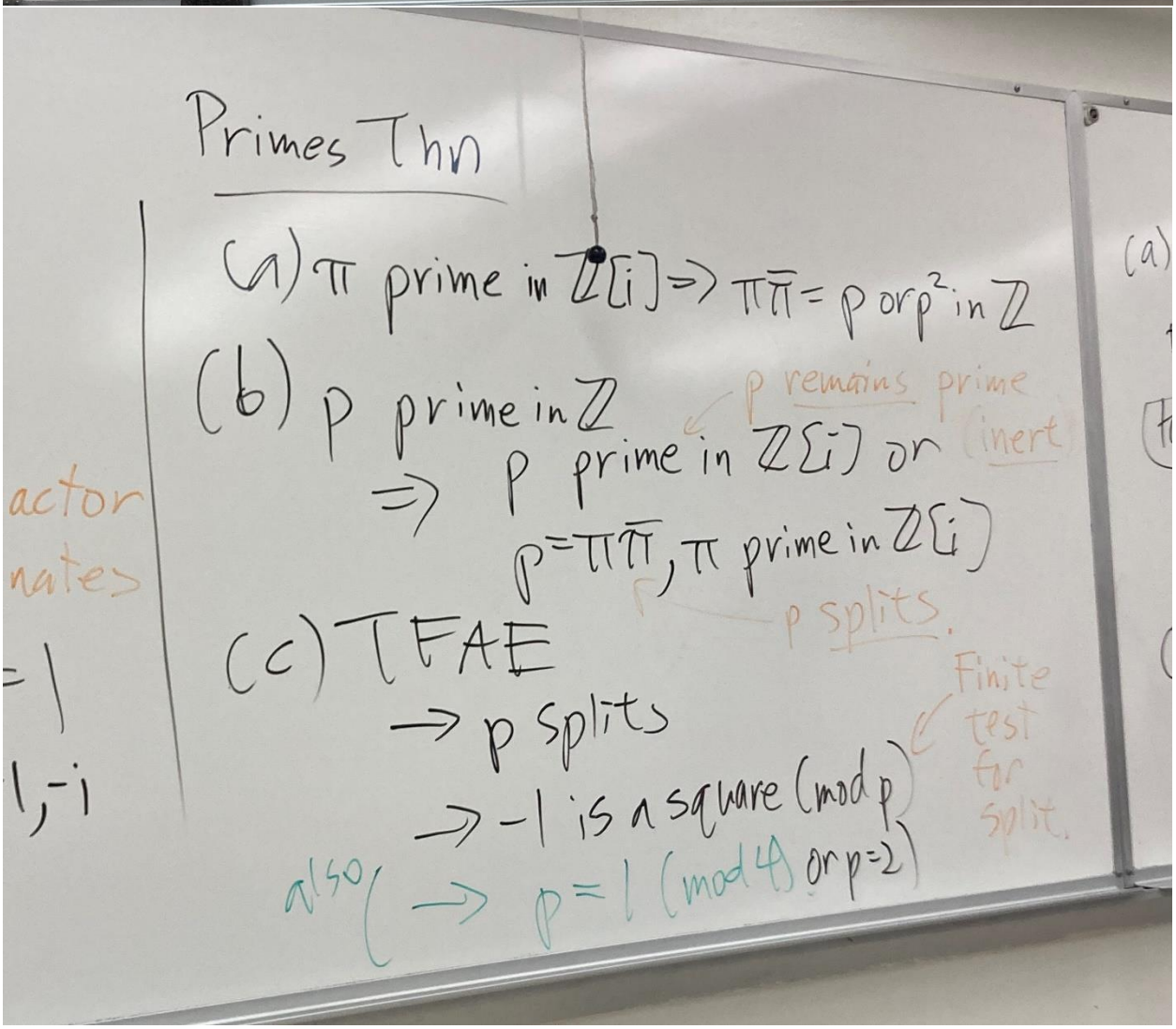
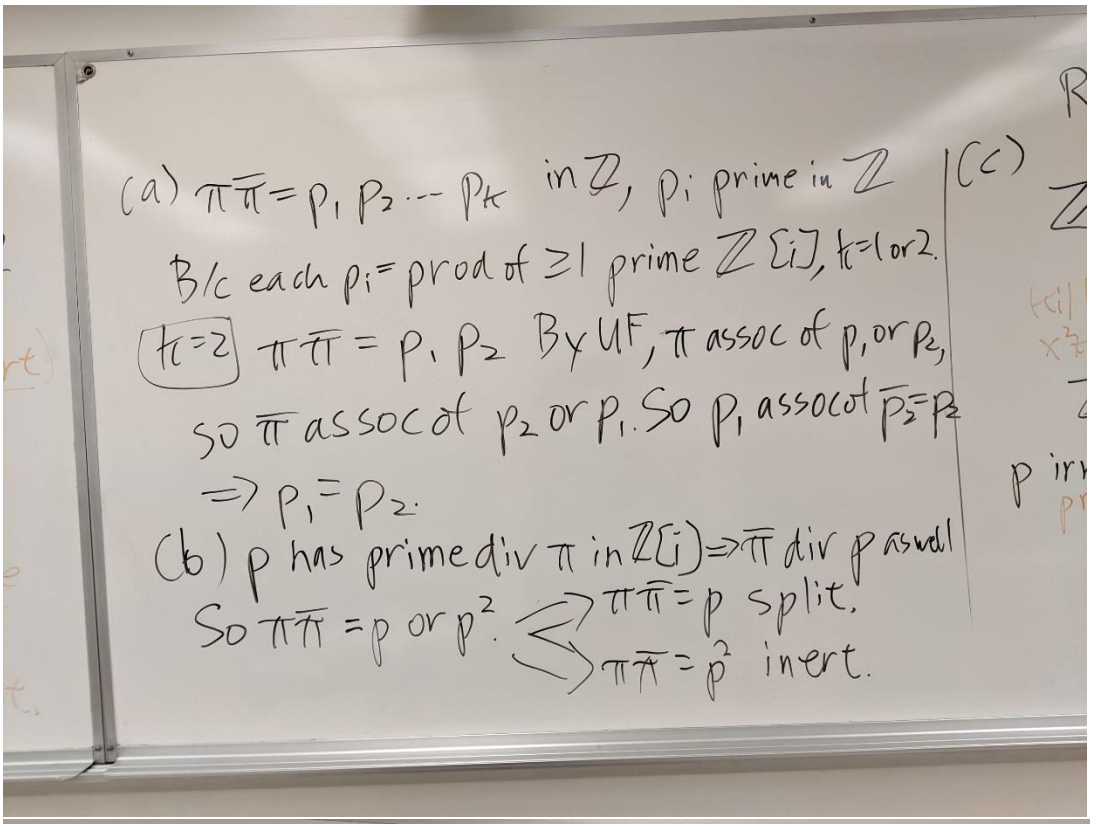
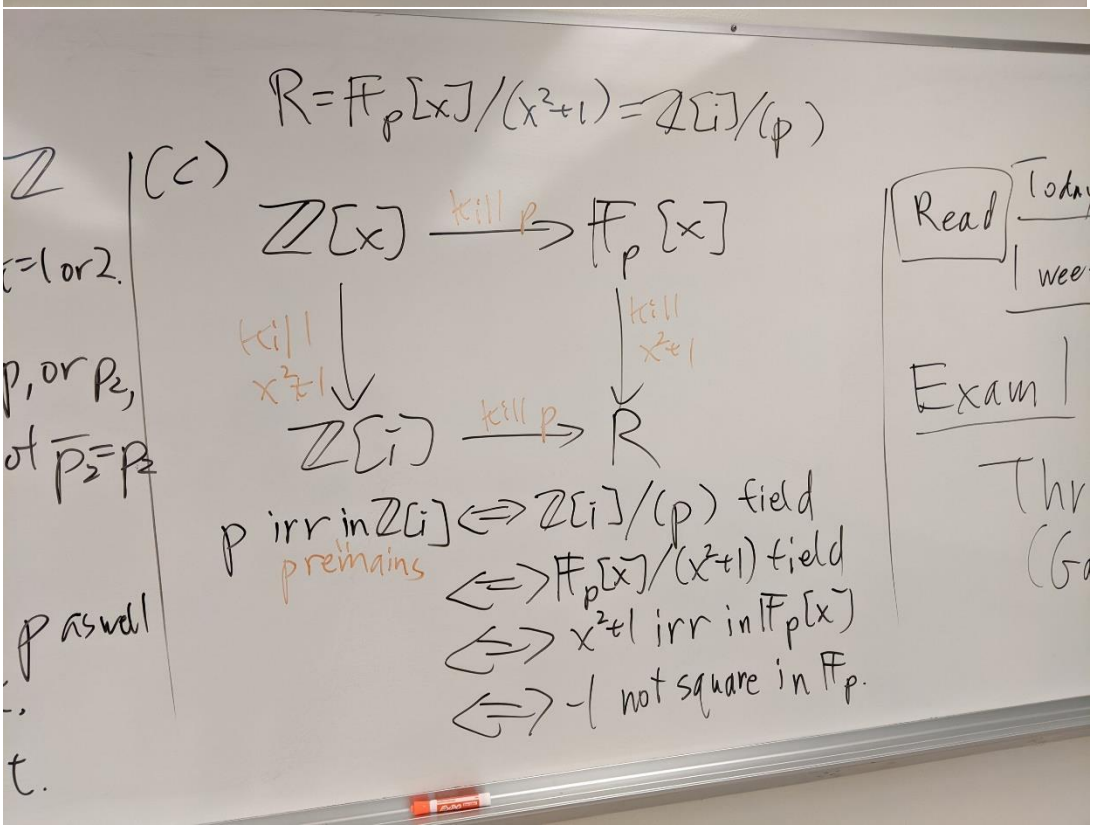
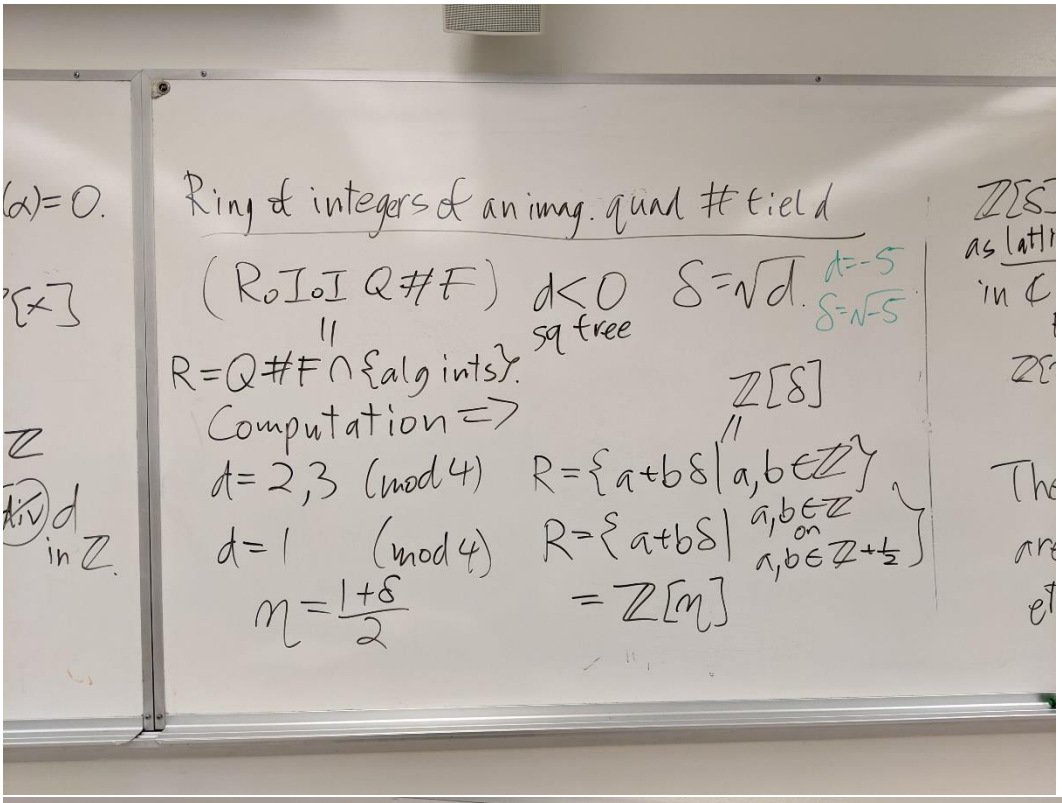
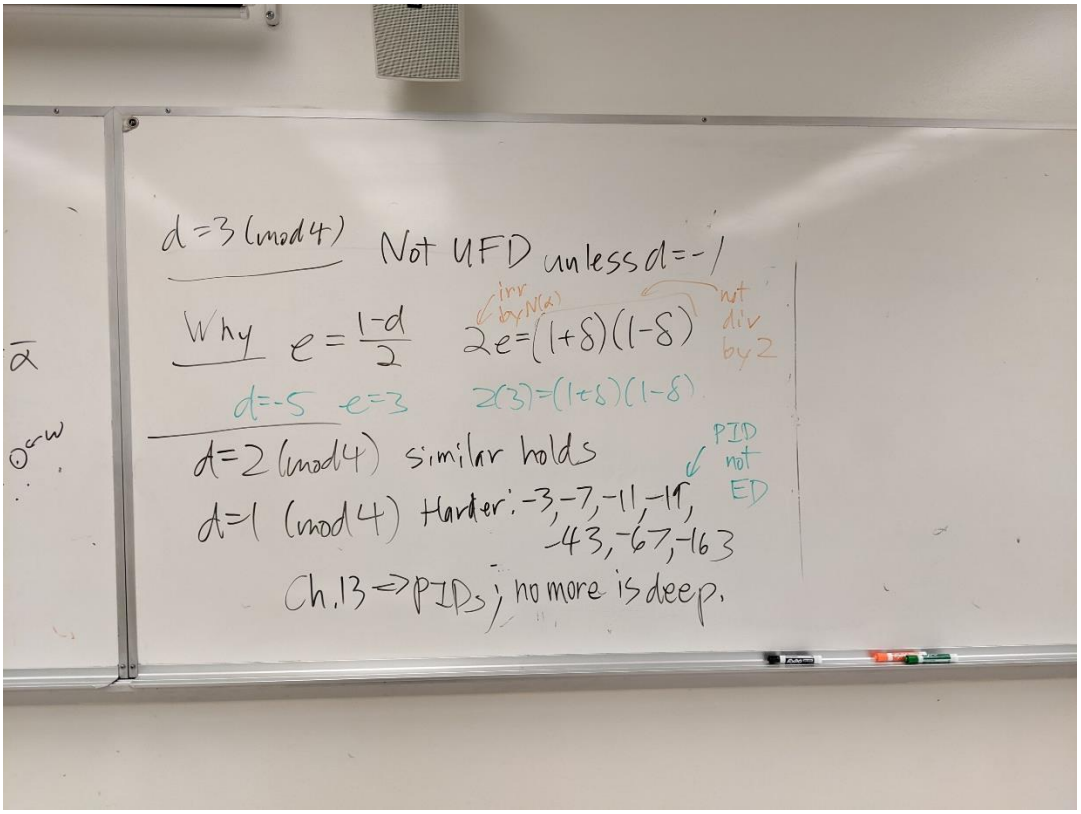

Important ideas from $\mathbb{Z}[i]$
$N(\alpha)$, $N(\alpha\beta)=N(\alpha)N(\beta)$
Remain / split
↳ ramify
Mod p test for remain/split (finite!)
Primes in $\mathbb{Z}[i]$
Def $z=a+bi$ $N(z)=N(a+bi)$
$=z\bar{z}=a^2+b^2\in\mathbb{Z}$
$N(zw)=N(z)N(w)$ ← so factor terminates
Also z unit in $\mathbb{Z}[i] \iff N(z)=1$
$\iff z=1,i,-1,-i$
Primes Th
(a) π pr
(b) p pr
$\Rightarrow$
(c) TF
$\rightarrow$
also(


Primes Thm
(a) π prime in $\mathbb{Z}[i] \Rightarrow \pi\bar{\pi} = p$ or p^2 in $\mathbb{Z}$
(b) p prime in $\mathbb{Z}$ ← p remains prime (inert)
$\Rightarrow$ p prime in $\mathbb{Z}[i]$ or
$p=\pi\bar{\pi}$, π prime in $\mathbb{Z}[i]$
p splits.
(c) TFAE
$\rightarrow$ p splits
$\rightarrow -1$ is a square (mod p) ← Finite test for split.
also($\rightarrow p=1 \pmod 4$ or $p=2$)
actor
nates>
=1
1,-i
(a)


(a) $\pi\bar{\pi} = p_1 p_2 \cdots p_k$ in $\mathbb{Z}$, p_i prime in $\mathbb{Z}$
B/c each p_i = prod of ≥ 1 prime $\mathbb{Z}[i]$, $k = 1$ or 2.
$k=2$ $\pi\bar{\pi} = p_1 p_2$ By UF, π assoc of p_1 or p_2,
so π assoc of p_2 or p_1. So p_1 assoc of $\bar{p}_2 = p_2$
$\Rightarrow p_1 = p_2$.
(b) p has prime div π in $\mathbb{Z}[i] \Rightarrow \bar{\pi}$ div p as well
So $\pi\bar{\pi} = p$ or p^2. $\Rightarrow \pi\bar{\pi} = p$ split.
$\Rightarrow \pi\bar{\pi} = p^2$ inert.
(c)


$R = \mathbb{F}_p[x]/(x^2+1) = \mathbb{Z}[i]/(p)$
(c)
$\mathbb{Z}[x]$ —kill p→ $\mathbb{F}_p[x]$
kill x^2+1
$\mathbb{Z}[i]$ —kill p→ R
p irr in $\mathbb{Z}[i]$ (p remains) $\Leftrightarrow \mathbb{Z}[i]/(p)$ field
$\Leftrightarrow \mathbb{F}_p[x]/(x^2+1)$ field
$\Leftrightarrow x^2+1$ irr in $\mathbb{F}_p[x]$
$\Leftrightarrow -1$ not square in $\mathbb{F}_p$.
Read
Exam


Ring of integers of an imag. quad # field
(R o I o I Q#F) d<0 sq free δ=√d. d=-5 δ=√-5
R=Q#F ∩ {alg ints}.
Computation =>
d=2,3 (mod 4) R={a+bδ | a,b∈ℤ}
d=1 (mod 4) R={a+bδ | a,b∈ℤ or a,b∈ℤ+½}
η=(1+δ)/2
=ℤ[η]
ℤ[δ]
as lattice in ℂ
Fundamental tile of ℤ[η]
ℤ[η] as lattice in ℂ (also black) index 2
Read
These in 13.3 to show there are 2 shapes of ideals in ℤ[δ], etc.


d=3 (mod 4) Not UFD unless d=-1
Why $e=\frac{1-d}{2}$
$2e=(1+\delta)(1-\delta)$
irr by N(a)
not div by 2
d=-5 e=3
2(3)=(1+δ)(1-δ)
d=2 (mod 4) similar holds
PID not ED
d=1 (mod 4) Harder: -3,-7,-11,-19,
-43,-67,-163
Ch.13 ⇒ PIDs; no more is deep.