6/15part2

Recall:

(1) $\mathbb{Z}[i] := \{a + bi | a, b \in \mathbb{Z}\}$is a unique factorization domain

(2) The units in $\mathbb{Z}[i]$ are± 1 and $\pm i$ $(i.e. a + bi$ with $a^2 + b^2 = 1)$

ex:
$p \equiv 1 \pmod 4$is a prime.show $p$is not a prime in $\mathbb{Z}[i]$
pf:
we know $p = a^2 + b^2 \neq 1$ for some $a, b \in \mathbb{Z}$
Then $p = (a + bi)(a - bi)$ is not a prime.
ex:
$p \equiv 3 \pmod 4$ is a prime.show p is a prime in $\mathbb{Z}[i]$
pf:
If $p = (a + bi)(c + di)\ in\ \mathbb{Z}[i], where\ a^2 + b^2 \neq 1\ and\ c^2 + d^2 \neq 1$
then $p^2 = p\overline{p} = (a + bi)(c + di)\overline{(a + bi)(c + di)} = (a^2 + b^2)(c^2 + d^2)$
then $p = a^2 + b^2 = c^2 + d^2$ a contradiction to $p \equiv 3 \pmod 4$
ex:
$p = a^2 + b^2 = 1 \pmod 4$ is a prime
show that $a + bi, a - bi$ are primes in $\mathbb{Z}[i]$
pf:suppose $a + bi = \alpha\beta$ for some $\alpha\beta \in \mathbb{Z}[i]$ not units
then $p = a^2 + b^2 = (a + bi)\overline{(a + bi)} = \alpha\beta\overline{\alpha}\overline{\beta} = (\alpha\overline{\alpha}(\beta\overline{\beta}))$
is factored into the product for two integers> 1 a contradiction.
ex:
$n \in \mathbb{Z}$ then $n = a^2 + b^2$ if and only if $n = 2^k m^2 p_1 p_2 \cdots p_t$
where $k, m, t \in \mathbb{N} \cup 0$ and $p_i \equiv 1 \pmod 4$ are primes.
$(\Leftarrow)$
$2 = 1^2 + 1^2$
$m^2 = m^2 + 0^2$
and $p_i = a_i^2 + b_i^2$ for some $a, b \in \mathbb{Z}$
$n^2 = a^2 + b^2$ for some $a, b \in \mathbb{Z}$
$(\Rightarrow)$
It suffices to show each prime $p \equiv 3 \pmod 4$ appears even times in n as factorization in $\mathbb{Z}$
we have $n = (a + bi)\overline{(a + bi)}$
since p is a prime in $\mathbb{Z}[i]$ the number it appears in $a + bi$ is the same as it appears in $\overline{a + bi}$.