

Read Herstein, Chapter 3, section 8, and Chapter 5, section 1.

1. From Herstein, do these problems:

- a) Chapter 3, section 8, page 152: #3(b), 6. [Hint for #6: see problem 4(a) on PS 2.]
- b) Chapter 3, supplementary problems, page 167: #1-3, 14. [Hint for #3: Try a principal ideal in a ring that's not a PID.]
- c) Chapter 5, section 1, page 214: #3.

2. a) Show that if $a \in \mathbb{Z}$ then a^2 is congruent to 0 or 1 mod 4.
b) Deduce that if $a, b \in \mathbb{Z}$ then $a^2 + b^2$ is not congruent to 3 mod 4.
c) For each of the following primes p , either write p in the form $a^2 + b^2$ or assert that this cannot be done. $p = 5, 7, 11, 13$.

3. Recall that if $\alpha = a + bi \in \mathbb{Z}[i]$ with $a, b \in \mathbb{Z}$, then the *norm* of α is $N(\alpha) = a^2 + b^2$.

- a) *From this definition*, show that $N(\alpha\beta) = N(\alpha)N(\beta)$ for $\alpha, \beta \in \mathbb{Z}[i]$.
- b) Deduce that if $\gamma \in \mathbb{Z}[i]$ and $N(\gamma)$ is a prime number in \mathbb{Z} , then γ is prime in $\mathbb{Z}[i]$.
- c) Show that if $p \in \mathbb{Z}$ is a prime number (in the usual sense), then $N(p) = p^2$, and each factor of p in $\mathbb{Z}[i]$ has norm equal to 1, p , or p^2 . [Hint: Part (a).]
- d) Deduce that for a prime number $p > 0$, p remains prime in $\mathbb{Z}[i]$ if and only if p has *no* factor of norm p .

4. Let $p > 0$ be prime in \mathbb{Z} . Prove that the following are equivalent:

- i) p does not remain prime in $\mathbb{Z}[i]$.
- ii) $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.
- iii) $p \not\equiv 3 \pmod{4}$.
- iv) $\exists \sqrt{-1} \in \mathbb{Z}/p$.

[Hint: First prove this for $p = 2$. Then for $p > 2$, prove each condition implies the next by using problem 3(d) and the definition of norm; problem 2(b); and problem 4(b) on Problem Set 6. For (iv) \Rightarrow (i), show $kp = a^2 + 1 = (a + i)(a - i)$ for some $k \in \mathbb{Z}$, and observe that p does not divide $a \pm i$.]