

1. Let $p > 2$ be a prime number, and let $f(x) = x^{\frac{p-1}{2}} - 1$.
 - a) Show that every square in $(\mathbb{Z}/p)^*$ is a root of $f(x) \in (\mathbb{Z}/p)[x]$.
 - b) Deduce that $f(x) = \prod_{i=1}^r (x - a_i)$, where f is as in (a) and where $\{a_1, \dots, a_r\}$ is the set of squares in $(\mathbb{Z}/p)^*$. [Hint: See PS 7 problem 7.]
 - c) Show that -1 is a square in $(\mathbb{Z}/p)^*$ if and only if $p \equiv 1 \pmod{4}$. [Hint: What is $f(-1)$?]
2.
 - a) Let $\alpha \in \mathbb{Z}[i]$. Show that if its norm $N(\alpha)$ is prime in \mathbb{Z} then α is prime in $\mathbb{Z}[i]$.
 - b) Show that the converse fails. [Hint: PS 7, problem 8.]
3. In $\mathbb{Z}[\sqrt{n}]$, define the *conjugate* of $\alpha = a + b\sqrt{n}$ to be $\bar{\alpha} = a - b\sqrt{n}$. Define the *norm* of α to be $N(\alpha) = \alpha\bar{\alpha} = a^2 - nb^2$.
 - a) Show that $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$ and that $N(\alpha\beta) = N(\alpha)N(\beta)$.
 - b) For which $n < 0$ is there a division algorithm in $\mathbb{Z}[\sqrt{n}]$, relative to $\alpha \mapsto N(\alpha)$?
4.
 - a) Show that $\mathbb{Z}[\sqrt{2}]$ has infinitely many units, whereas $\mathbb{Z}[\sqrt{-2}]$ has only finitely many. [Hint: For $\mathbb{Z}[\sqrt{2}]$, consider $u = 1 + \sqrt{2}$. For $\mathbb{Z}[\sqrt{-2}]$, consider norms (as in problem 3) or absolute values.]
 - b) Can you make a general conjecture about the number of units in $\mathbb{Z}[\sqrt{n}]$?
5. Let $p > 0$ be a prime number in \mathbb{Z} .
 - a) Show that if $p \equiv 1 \pmod{4}$ then p is not prime in $\mathbb{Z}[i]$, but instead splits as the product of two distinct primes. [Hint: By problem 1(c), $p|(a^2 + 1)$ for some a ; if p remained prime in $\mathbb{Z}[i]$ show $p|a \pm i$ and obtain a contradiction. For the second assertion, use norms.]
 - b) Show that if $p \equiv 3 \pmod{4}$ then p remains prime in $\mathbb{Z}[i]$. [Hint: If $p = \alpha\beta$, then $N(\alpha) = p$. Can p be the sum of two squares?]
 - c) Show that if $p = 2$ then up to a unit, p is the square of a prime in $\mathbb{Z}[i]$.
6. Suppose α is prime in $\mathbb{Z}[i]$, and let $p_1 \cdots p_r$ be the prime factorization of $N(\alpha)$ in \mathbb{Z} .
 - a) Show that $\alpha|p_j$ for some j .
 - b) Deduce that if $\alpha \notin \mathbb{Z} \cup i\mathbb{Z}$, then $N(\alpha)$ is prime. [Hint: Show $p_j = \alpha\beta$ with neither factor a unit, and then take norms.]
7. Show that $\alpha \in \mathbb{Z}[i]$ is prime if and only if either
 - (i) $\alpha = \varepsilon p$ where $\varepsilon \in \{\pm 1, \pm i\}$ and $p > 0$ is a prime in \mathbb{Z} with $p \equiv 3 \pmod{4}$; or
 - (ii) $N(\alpha)$ is prime in \mathbb{Z} .
 [Hint: Use problems 5 and 6.] Compare with your computations in PS 7 problem 8.
8. Let R be a commutative ring.
 - a) Let I_1, \dots, I_n be ideals in R , and let $\mathfrak{p} \subset R$ be a prime ideal containing $I_1 \cap \cdots \cap I_n$. Show that $I_i \subset \mathfrak{p}$ for some i .
 - b) Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be prime ideals in R , and let $I \subset R$ be an ideal that is contained in $\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$. Show that $I \subset \mathfrak{p}_i$ for some i . [Hint: Induction on n .]
 - c) Explain the content of (a) and (b) geometrically.