Math 602 Problem Set #9 Due Mon., Nov. 15, 2021

1. Let $p > 2$ be a prime number, and let $f(x) = x^{\frac{p-1}{2}} - 1$.

a) Show that every square in $(\mathbb{Z}/p)^\times$ is a root of $f(x) \in (\mathbb{Z}/p)[x]$.

b) Deduce that $f(x) = \prod_{i=1}^{r}(x - a_i)$, where $\{a_1, \dots, a_r\}$ is the set of squares in $(\mathbb{Z}/p)^\times$. [Hint: See PS 8 problem 5.]

c) Show that -1 is a square in $(\mathbb{Z}/p)^\times$ if and only if $p \equiv 1 (\bmod 4)$. [Hint: $f(-1) = ?$]

2. a) Which of the following elements of $\mathbb{Z}[i]$ can be factored non-trivially? For each one that can be, do so explicitly. $2, 3, 5, 7, 11, 13, 15, 3i, 5i, 2+i, 3+i$

b) Let $\alpha \in \mathbb{Z}[i]$. Recall that its norm is $N(\alpha) = \alpha\bar{\alpha}$. Show that if $N(\alpha)$ is prime in $\mathbb{Z}$ then α is prime in $\mathbb{Z}[i]$.

c) Show that the converse fails. [Hint: part (a).]

3. Let $p > 0$ be a prime number in $\mathbb{Z}$.

a) Show that if $p \equiv 1 \,(\bmod 4)$ 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 $p \equiv 3 \,(\bmod 4)$ 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 multiplication by a unit, p is the square of a prime in $\mathbb{Z}[i]$.

4. 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.]

5. 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 $p \equiv 3 \,(\bmod 4)$; or

(ii) $N(\alpha)$ is prime in $\mathbb{Z}$.

[Hint: Use problems 3 and 4.] Compare with your computations in problem 2(a).