Homework Assigment 13

Due Friday, May 7

1. Let R be a unique factorization domain.
   (a) Fix $r \in R$. Show that r is irreducible if and only if it is prime.
   (b) Let $a, b \in R$. Show that a greatest common denominator of a and b exists, and is unique up to multiplication by a unit.
2. Let's turn our attention to $\mathbb{Z}[\sqrt{-5}]$.
   (a) Show that 3 is an irreducible element but not a prime element of $\mathbb{Z}[\sqrt{-5}]$.
   (b) Deduce from part (a) that $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain. Explain why this means $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain.

   We now know abstractly that $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain. Let's exhibit an explicit nonprincipal ideal.

   (c) Let $\mathfrak{p} \subseteq \mathbb{Z}[\sqrt{-5}]$ be any prime ideal containing 3. Prove that $\mathfrak{p}$ cannot be principal.
   (d) Prove that the ideal $I = (3, 2+\sqrt{-5})$ is a maximal ideal of $\mathbb{Z}[\sqrt{-5}]$ containing 3. Conclude that it cannot be principal. (*Hint:* Show $\mathbb{Z}[\sqrt{-5}]/(3)$ has 9 elements and $I/(3)$ has 3 elements. Then leverage the third isomorphism theorem for rings to compute $\mathbb{Z}[\sqrt{-5}]/I$.)
3. Let R be a Euclidean domain, and $N : R \to \mathbb{Z}_{\geq 0}$ a Euclidean norm. Let's explore how the norm can help us characterize the units in R.
   (a) Let $m = \min\{N(x) : x \neq 0\}$. Show that if $N(x) = m$, then $x \in R^\times$.
   (b) Let $\hat{N} : R \to \mathbb{Z}$ be given by the following rule.

   $$\hat{N}(r) = \min_{x \in R \setminus \{0\}} N(xr).$$

   Prove that $\hat{N}$ is a Euclidean norm on R, and also that it satisfies the further condition that if $a|b$ then $\hat{N}(a) \leq \hat{N}(b)$.
   (c) Prove that $x \in R^\times$ if and only if $\hat{N}(x) = \hat{N}(1)$.
4. Let R be a principal ideal domain.
   (a) Show that if $\mathfrak{p}$ is a prime ideal, then $R/\mathfrak{p}$ is also a principal ideal domain.
   (b) Show that if S is a multiplicative subset not containing 0, then $S^{-1}R$ is a principal ideal domain.
5. Let p a prime number so that $p \equiv 3 \mod 4$.
   (a) Prove that p generates a maximal ideal of $\mathbb{Z}$.
   (b) Show that $\mathbb{Z}[i]/(p)$ is a field with p^2 elements. Denote it by $\mathbb{F}_{p^2}$.
   (c) Explain why $\mathbb{F}_{p^2} \not\cong \mathbb{Z}/p^2\mathbb{Z}$.
   (d) Prove that there is an injective homomorphism $\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^2}$.