Homework 9 : Due Wednesday, April 25

Problem 1: Let $K = \mathbb{Q}(\sqrt{-3})$. Notice that $-3 \equiv 1 \pmod 4$, so $\mathbb{Z}[\sqrt{-3}] \subsetneq \mathcal{O}_K$. We know from problem 4 that $\mathbb{Z}[\sqrt{-3}]$ is not a PID (because it is not a UFD) but we know from class that $\mathcal{O}_K$ is a PID (because it is a Euclidean domain).
a. Working in $\mathbb{Z}[\sqrt{-3}]$, let $I = \langle 2, 1+\sqrt{-3}\rangle$. Show that I is a nonprincipal ideal.
b. Working in $\mathcal{O}_K$, let $J = \langle 2, 1+\sqrt{-3}\rangle$. We know that J must be a principal ideal. Find a generator for J.

Problem 2: Let Let $p \in \mathbb{N}^+$ be prime, let $d \in \mathbb{Z}$ be square-free, and suppose that $p \nmid d$.
a. Show that if there exist $a, b \in \mathbb{Z}$ with $p = |a^2 - db^2|$, then d is a quadratic residue modulo p.
b. Suppose that $\mathbb{Z}[\sqrt{d}]$ is a UFD. Show that the converse to part a holds, i.e. show that if d is a quadratic residue modulo p, then there exist $a, b \in \mathbb{Z}$ with $p = |a^2 - db^2|$.
Note: This generalizes our results about which primes are sums of squares (corresponding to $d = -1$). It also gives added motivation to understand quadratic residues. Moreover, the proof of part b can be generalized to work in the case where $d \equiv 1 \pmod 4$ and $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a UFD (though don't bother writing that up). This allows one to handle a few more values of d beyond those in part b, including $d = -3$.

Problem 3: Let $p \in \mathbb{N}^+$ be an odd prime.
a. Show that a primitive root modulo p must be a quadratic nonresidue modulo p.
b. Show that every quadratic nonresidue modulo p is a primitive root modulo p if and only if $p = 2^n + 1$ for some $n \in \mathbb{N}^+$. Such primes are called *Fermat primes* and in fact any such prime must be of the form $2^{2^k}+1$.

Problem 4: Suppose that $p \in \mathbb{N}^+$ is an odd prime. Determine what the product of the quadratic residues in the set $\{1, 2, \dots, p-1\}$ is congruent to modulo p.

Problem 5: Suppose that $p \in \mathbb{N}^+$ is an odd prime. Determine what the sum of the quadratic residues in the set $\{1, 2, \dots, p-1\}$ is congruent to modulo p.
Note: $p = 3$ is special.

Problem 6: Let $p \in \mathbb{N}^+$ be an odd prime and let $k \in \mathbb{N}^+$. Let $a \in \mathbb{Z}$ with $p \nmid a$.
a. Show that a is a quadratic residue modulo p^k if and only if $a^{\varphi(p^k)/2} \equiv 1 \pmod{p^k}$.
b. Show that a is a quadratic residue modulo p^k if and only if a is a quadratic residue modulo p.