Homework #9. Due Tuesday, April 22nd, by 4pm

Reading:

1. For this homework assignment: Chapter 10, Sections 10.1-10.3 + class notes (Lectures 16-17)

2. For the next week's classes: TBA

Problems:

1. Recall that for a prime p and a nonzero integer n, by $ord_p(n)$ we denote the largest power of p which divides n. Assume now that p is a prime of the form $4k + 3$

(a) Prove that if $p \nmid a$ or $p \nmid b$, then $p \nmid (a^2 + b^2)$. **Hint:** Assume that $a^2 + b^2 = pk$, rewrite this equation in a suitable way and then use Legendre symbols to get a contradiction.

(b) Use (a) to prove that $ord_p(a^2 + b^2)$ is even for any $a, b \in \mathbb{Z}$ with $a \neq 0$ or $b \neq 0$. This completes the proof of theorem characterizing which integers are representable as sums of two squares.

2. Let ω be a complex number such that $\omega \notin \mathbb{Z}$ and $\omega^2 = n_1\omega + n_2$ for some $n_1, n_2 \in \mathbb{Z}$. For instance, if d is a positive integer which is not a perfect square, we can take $\omega = \sqrt{d}$ or $\omega = i\sqrt{d}$. Define

$$\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\} \quad \text{and} \quad \mathbb{Q}[\omega] = \{a + b\omega : a, b \in \mathbb{Q}\}.$$

(a) Prove that $\mathbb{Z}[\omega]$ is a commutative ring with 1 and that $\mathbb{Q}[\omega]$ is a field.

For the remaining parts of this problem assume that $\omega = \sqrt{d}$ or $\omega = i\sqrt{d}$ for some d as above.

(b) Define the conjugation map $\iota : \mathbb{Q}[\omega] \to \mathbb{Q}[\omega]$ by $\iota(a + b\omega) = a - b\omega$ Prove that ι is a ring isomorphism.

(c) Prove that $u \cdot \iota(u) \in \mathbb{R}$ for any $u \in \mathbb{Q}[\omega]$.

(d) Define the norm map $N : \mathbb{Q}[\omega] \to \mathbb{R}_{\geq 0}$ by $N(u) = |u \cdot \iota(u)|$. Prove that $N(uv) = N(u)N(v)$.

(e) Prove that $N(u) \in \mathbb{Z}$ for any $u \in \mathbb{Z}[\omega]$ and $N(u) = 0 \iff u = 0$.

(f) Let $u \in \mathbb{Z}[\omega]$. Prove that $N(u) = 1 \iff u$ is a unit of $\mathbb{Z}[\omega]$.

3. Prove that $\mathbb{Z}[i\sqrt{2}]$ is a Euclidean domain.

4.

(a) Determine which primes are representable in the form $a^2 + 2b^2$ with $a, b \in \mathbb{Z}$. **Hint:** first test all primes up to, say, 50, to make a conjecture. To prove the conjecture use Problem 3 for the positive direction (primes which can be represented) – this is very similar to what we did in class – and then a suitable analogue of Problem 1 for the negative direction (primes which cannot be represented).

(b) (bonus) Describe all integers representable as $a^2 + 2b^2$ with $a, b \in \mathbb{Z}$.

5. Let $R = \mathbb{Z}[\sqrt{5}]$. Prove that 2 considered as an element of R is irreducible but not prime. **Hint:** To prove that 2 is not prime find two non-equivalent factorizations of 4 in R. To prove that 2 is irreducible argue by contradiction and use the norm function from Problem 2.

6. Exercise 10.10 from the book.