Homework #6, to be completed by Thursday, October 20th

Reading:

1. For this homework assignment: Sections 7.5,7.6, the beginning of 10.2 and class notes from Lecture 14.

2. For the next week's classes: Sections 10.1-10.4.

Problems:

1. Let p be an odd prime, let $a \in \mathbb{Z}$ be coprime to p, and let $k \geq 1$ be an integer. Use the lifting method to prove that a is a quadratic residue mod $p^k \iff a$ is a quadratic residue mod p. Note that a completely different (group-theoretic) proof of this fact is given in the book (Theorem 7.13)

Note: Make sure to read 7.5 and 7.6 before solving problems 2 and 4 (this material was not discussed in class).

2. Let Q_n be the group of quadratic residues mod n (in this problem we think of quadratic residues as elements of U_n, not as integers, which is the convention that the book uses).

(a) Let n be an odd integer. Prove that $|Q_n| = \frac{\phi(n)}{2^k}$ where k is the number of distinct prime divisors of n.

(b) Prove that Q_{105} is a cyclic group of order 6.

(c) Find a generator for Q_{105}.

3. Exercise 7.20 from the book.

4. Exercise 7.21 from the book.

5. Use the Euclidean algorithm to find $gcd(7+3i, 3+i)$ in $\mathbb{Z}[i]$

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

7. 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 $\mathbb{Z}[\omega]$.