Name: ______________________________

Read the notes, "Prerequisites for Chapter 8," and the parts of the textbook referenced therein. Focus on the first two sections of the notes.

Reading Questions

1. (a) List the four units in $\mathbb{Z}[i]$.

   (b) Find the four associates of $2 + i$ in $\mathbb{Z}[i]$.

2. The definition of an associate of an element in $\mathbb{Z}[i]$ is given explicitly. State a suitable modification of this definition to define an associate of an element of $\mathbb{Z}[\omega]$.

3. The definition of a prime element in $\mathbb{Z}[i]$ is given explicitly. State a suitable modification of this definition to define a prime element of $\mathbb{Z}[\omega]$.

4. In your own words, explain the notations:

   (a) $\mathbb{R}[x]$

(b) $\mathbb{Z}[x]$

(c) $\mathbb{F}_p$

5. Why does the statement "$\overline{3} \cdot \overline{2} = \overline{3} \cdot \overline{4}$ but $\overline{2} \neq \overline{4}$ in $\mathbb{Z}/6$" show that $\mathbb{Z}/6$ is *not* a domain?

6. What struck you in this reading? What is still unclear? What remaining questions do you have?

Name: ____

Read the introduction to Chapter 8 and Section 8.1. Focus on the concrete aspects pertaining to $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$; in particular you may skim or omit the part on abstract Euclidean domains, as long as you do read Example 8.9.

Reading Questions

1. The introduction to Chapter 8 gives the motivation for studying arithmetic in rings of cyclotomic integers and gives an overview of Chapter 8. Briefly summarize the motivation in your own words.

Section 8.1 describes the Division Algorithm and the Euclidean Algorithm in $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ and describes a more general structure (called a Euclidean Domain) that captures the properties shared by $\mathbb{Z}$, $k[x]$ (where k is a field), $\mathbb{Z}[i]$, and $\mathbb{Z}[\omega]$ which are necessary for the Division Algorithm and Euclidean Algorithm to work.

2. Reread Examples 8.1 and 8.3 carefully, working out the computations for yourself by hand on scratch paper. Understanding these examples will shed light on the results in the rest of the section.

   (a) Illustrate Example 8.1 by plotting the Gaussian integers in the complex plane, along with w/z and q.

   (b) Illustrate Example 8.3 by plotting the Gaussian integers in the complex plane, along with w/z and all four choices of q.

   (c) Reread the proof of Proposition 8.2 with these examples in mind.

3. Illustrate Example 8.5 by plotting the Eisenstein integers in the complex plane, along with w/z and q. Reread the proof of Proposition 8.4 with this example in mind.

4. Reread Example 8.9. What is the gcd of $91 + 84\omega$ and $34 + 53\omega$ in $\mathbb{Z}[\omega]$ that is computed in this example? What are the associates of this gcd in $\mathbb{Z}[\omega]$?

5. What struck you in this reading? What is still unclear? What remaining questions do you have?

Math 221, 8.2-I Primes Upstairs and Primes Downstairs: Gaussian Primes

Name: ______________________________

Read Section 8.2, pages 337-343.

Reading Questions

1. Study Example 8.12. A careful reading of this example will help the results in this section make more sense. What is the prime factorization of $-211 + 102i$ in $\mathbb{Z}[i]$? How do we know that the factors are prime in $\mathbb{Z}[i]$? (Cite a proposition.)

2. There are many new terms in this section. Make sure to take notes on them. In particular, make sure you understand what is meant by primes **upstairs** and primes **downstairs**, **rational prime**, **rational integer**, and a Gaussian prime **lying above** a rational prime.

3. A prime $p \in \mathbb{Z}$ may factor in $\mathbb{Z}[i]$ or it may remain prime in $\mathbb{Z}[i]$. Give an example of each.

4. Let p be a rational prime. State four conditions equivalent to "p factors in $\mathbb{Z}[i]$."

5. A rational prime exhibits one of the following three behaviors in $\mathbb{Z}[i]$: it **splits**, it is **inert**, or it **ramifies**. In your notes, make sure to describe what each of these terms means. Give an example of each type of behavior here.

6. The main results in this reading are Theorem 8.21 (Law of Decomposition of Gaussian Integers) and Corollary 8.22 (Classification of Gaussian Primes.) Write these in your notebook, word for word.

7. The primes in $\mathbb{Z}[i]$ are of three types (as described in Corollary 8.22). Give an example of each type.

8. What struck you in this reading? What is still unclear? What remaining questions do you have?

Math 221, 8.2-II Primes Upstairs and Primes Downstairs: Eisenstein Primes

Name: ________________________________

Read Section 8.2, pages 344-348.

Reading Questions

1. Let p be a rational prime. State three conditions equivalent to "p factors in $\mathbb{Z}[\omega]$."

2. A rational prime either splits, is inert, or ramifies in $\mathbb{Z}[\omega]$. Give an example of each.

3. The main results in this reading are Theorem 8.29 (Law of Decomposition of Eisenstein Integers) and Corollary 8.30 (Classification of Eisenstein Primes.) Write these in your notebook, word for word.

4. The primes in $\mathbb{Z}[\omega]$ are of three types (as described in Corollary 8.30). Give an example of each type.

5. What struck you in this reading? What is still unclear? What remaining questions do you have?

Math 221, 8.3 Fermat's Last Theorem for Exponent 3

Name: ______________________________

Read Section 8.3. Read for the big picture, and be careful not to get embroiled in the details!

Reading Questions

1. Reread the "How to Think About It" box at the bottom of page 349, and summarize it.

2. There are three (or four) important preliminaries (a proposition, a lemma, and a definition, with a proposition.) What are they?

3. If $z = 1 + 16\omega = (-1)(5 - \omega)(1 - \omega)^2$, what is $\nu(z)$?

4. What is "the first case"? What is "the second case"?

5. Gauss' proof of the second case follows from a more general theorem. State this theorem.

6. What struck you in this reading? What is still unclear? What remaining questions do you have?