Study guide

- Know the definition of the Gaussian integers $\mathbb{Z}[i]$, and how to do arithmetic with them.
- What is the *norm* $N(a+bi)$ of a Gaussian integer $a+bi$?
- How do you prove that primes $p \equiv 3 \bmod 4$ are not sums of two squares?
- How do you perform the *division algorithm* in $\mathbb{Z}[i]$?
- Understand the *descent procedure* showing that primes $p \equiv 1 \bmod 4$ are sums of two squares.
- Which positive integers (prime or otherwise) are sums of two squares?

1. (Textbook 24.1(a))
   Make a list of all primes $p < 50$ that can be written in the form $p = a^2+ab+b^2$. For example, $p = 7$ has this form with $a = 2$ and $b = 1$, while $p = 11$ cannot be written in this form. Try to find a pattern and make a guess as to exactly which primes have this form. (Can you prove that at least part of your guess is correct?)

2. (Textbook 24.2)
   If the prime $p \neq 5$ can be written in the form $p = a^2 + 5b^2$, show that
   $$p \equiv 1 \text{ or } 9 \bmod 20.$$

3. (Textbook 24.3)
   Staring from the equation $557^2 + 55^2 = 26 \cdot 12049$, apply the descent procedure (either the version in $\mathbb{Z}[i]$ to be shown in class on Friday, or the method as described on p. 187) to write the number 12049 as a sum of two squares.

4. (Textbook 25.1)
   For each number, either write the number as a sum of two squares or explain why it is not possible to do so. *Hint: begin by factoring the number into primes.*
   a) 4370 b) 1885
   c) 1189 d) 3185

5. (Optional bonus, for a small amount of extra credit.) This problem explains an alternative proof that any prime $p \equiv 1 \bmod 4$ is a sum of two squares, based on an adaptation of the Euclidean algorithm to the Gaussian integers $\mathbb{Z}[i]$. To prove these facts, you may want to revisit the arguments made in §6, for which these are $\mathbb{Z}[i]$-analogs.
   (a) Suppose that z, w are two Gaussian integers. Denote by $\langle z, w\rangle$ the set
   $$\langle z, w\rangle = \{uz + vw : \ u, v \in \mathbb{Z}[i]\}.$$
   This is the analog of the set of "integer linear combinations" we considered while studying the Euclidean algorithm. Prove that if $x \in \langle z, w\rangle$, then the remainder (as defined in class for $\mathbb{Z}[i]$) when x is divides by z (or w) is also in $\langle z, w\rangle$.
   (b) Suppose that z, w are two nonzero Gaussian integers. Let $g \in \langle z, w\rangle$ be a nonzero element of $\langle z, w\rangle$ such that the norm $N(g)$ is as small as possible. Prove that $g \mid z$ and $g \mid w$, i.e. g is a (Gaussian) *common divisor* of z and w. We will call such an element g a *greatest common divisor* of z and w. (You may want to see if you prove that it is indeed the "greatest" common divisor in a suitable sense, but you don't need to do so in this problem.)

(c) Now suppose that $p \in \mathbb{Z}$ is an (ordinary) prime, and a, b are integers such that $p \mid a^2+b^2$ but $p^2 \nmid a^2 + b^2$. Prove that, if $g \in \langle p, a+bi\rangle$ is a greatest common divisor of p and $a + bi$, then $N(g) = p$.

In particular, this argument shows that p is a sum of two squares: if $g = u + iv$, $u, v \in \mathbb{Z}$, then $N(g) = u^2 + v^2 = p$.