Review

1. What does it mean for $a | b$ (“$a$ divides $b$”), where $a$ and $b$ are integers?

2. What is the gcd of integers $a$ and $b$ (written $\text{gcd}(a, b)$)?

3. Show that $\text{gcd}(a, b) = \text{gcd}(a, b - a)$.

4. (Division Algorithm) Show that if $a, b \in \mathbb{Z}$ ($b \neq 0$) then there are unique integers $q$ and $r$ ($0 \leq r < |b|$) such that $a = b \cdot q + r$ (Prop 1.1.11).

Euclid’s Lemma & the Fundamental Theorem

1. (a) Let $a = 7, b = 3$. Find $q$ and $r$ from the Division Algorithm.

   (b) Let $a = -7, b = 3$. Find $q$ and $r$ from the Division Algorithm.

   (c) Let $a = 25, b = -3$. Find $q$ and $r$ from the Division Algorithm.

2. (Euclid’s Lemma) Show that, if $p$ is prime and $p | ab$ then $p | a$ or $p | b$.

3. Show that every natural number $n > 1$ is a product of primes.

4. (Fundamental Theorem of Arithmetic) Show that every natural number is a unique product of primes.

Chapter 2

5. What is a ring?

6. Explain why $\mathbb{Z}[\sqrt{-5}] = a + b\sqrt{-5} : a, b \in \mathbb{Z}$ is a ring (p.3).

7. Show that $\mathbb{Z}[\sqrt{-5}]$ does not have unique factorization.