(1) The main point of Chapter 5 is the Fundamental Theorem of Arithmetic, which usually refers to the combination of the textbook’s Theorems 5.2 and 5.5. The book gives this as two separate theorems because the theorem as usually stated has an existence part and a uniqueness part, and they need to be proved separately. Most of you will have seen the Fundamental Theorem (and a proof very much like the proofs of Theorems 5.2 and 5.5 in the book) in Math 300.

(2) The existence part is proved by induction, using the version of induction called “strong induction” or (in the Math 300 textbook, at least) “the second principle of mathematical induction”. The proof basically says you can keep factoring a number until you get to primes.

(3) The uniqueness part is proved by induction, but it depends on a key result about primes called Euclid’s Lemma (Theorem 5.6 in the textbook), which says that if a prime $p$ divides a product $bc$ of integers, then $p$ divides $b$ or $c$. We usually prove Euclid’s Lemma using Bézout’s theorem (though that’s not how Euclid proved it).

(4) In fact, Euclid’s Lemma characterizes primes (in the integers). In other words, an integer $p \neq 1, -1$ is a prime (in the sense of not having any nontrivial factorization) if and only if it satisfies Euclid’s Lemma. Or, to put it another way, the only integers that satisfy Euclid’s Lemma are the primes and $\pm 1$. (Obviously, 1 and $-1$ divide all integers, so they trivially satisfy Euclid’s Lemma.) The converse of Euclid’s Lemma is easy to prove:

**Proposition.** Suppose $n$ is a positive integer that satisfies the condition that, whenever $b$ and $c$ are integers with $n \mid bc$, $n \mid b$ or $n \mid c$. Then $n$ is a prime.

**Proof.** Suppose $n = xy$ is a nontrivial factorization of $n$, so $x, y$ are positive integers with $x, y > 1$. So we have $1 < x, y < n$. But clearly $n \mid xy$, so $n \mid x$ or $n \mid y$, which says that $n \leq x$ or $n \leq y$. This is a contradiction, so no nontrivial factorization of $n$ exists. □

(5) So we have two reasonable definitions of prime: no nontrivial factorizations, and satisfying Euclid’s Lemma. In $\mathbb{Z}$ these give us (excluding $\pm 1$), the same elements. And we need both of these definitions to prove the Fundamental Theorem of Arithmetic. But in other rings (formal definition coming later!) that look a lot like $\mathbb{Z}$, these two notions of prime are not equivalent. Here’s a sketch of a standard example.

Let $R$ be the set of complex numbers of the form $x + y\sqrt{-5}$, where $x, y \in \mathbb{Z}$. We have the obvious addition and multiplication operations on $R$. Define a norm $\mathcal{N} : R \to \mathbb{Z}$ by $\mathcal{N}(x + y\sqrt{-5}) = x^2 + 5y^2$. (This is just the usual complex norm, restricted to the subset $R$ of $\mathbb{C}$.) It’s easy to see that $\mathcal{N}(rs) = \mathcal{N}(r)\mathcal{N}(s)$. This fact implies that the only elements of $R$...
that have multiplicative inverses are 1 and −1 (they’re the only elements of norm 1, and if an element r has a multiplicative inverse s, we’d have \( N(r)N(s) = 1 \) so \( N(r) = N(s) = 1 \)).

We can use the norm to show that certain elements of \( R \) have no nontrivial factorizations (meaning, as usual, that neither factor is ±1). For instance, consider \( 2 = 2 + 0\sqrt{-5} \). We see that \( N(2) = 4 \). If \( 2 = rs \) is a nontrivial factorization, then \( N(r)N(s) = 4 \) and, since the factorization is nontrivial, we’d need to have \( N(r) = N(s) = 2 \). But there are no elements in \( R \) of norm 2. Similarly, we can show that \( 3 \) has no nontrivial factorizations.

Now consider \( a = 1 + \sqrt{-5} \) and \( b = 1 - \sqrt{-5} \). We see that \( N(a) = N(b) = 6 \). So if \( a \) has a nontrivial factorization \( a = rs \), then we must have one of \( r \) and \( s \) having norm 2 and the other having norm 3. But there are no elements of norm 2 or norm 3 in \( R \), so this says \( a \) has no nontrivial factorizations. A similar argument applies to \( b \).

Now observe that \( 2 \cdot 3 = a \cdot b = 6 \). So \( 2 \mid ab \). But it’s clear that \( 2 \) does not divide \( a \) or \( b \)—if it did, we’d have \( 2 \mid 1 \). So in \( R \), the element \( 2 \) satisfies the “no nontrivial factorizations” definition of prime, but not the “Euclid’s Lemma” definition of prime. In particular, if we take the “no nontrivial factorizations” definition, then the uniqueness part of the Fundamental Theorem of Arithmetic does not hold in \( R \); there can be fundamentally different factorizations into “primes.”

So if we’re going to work in rings other than \( \mathbb{Z} \), we should have separate names for these two notions (even though they coincide in \( \mathbb{Z} \)). The standard terminology is to say that elements that don’t have any nontrivial factorizations are irreducible and that elements that satisfy Euclid’s Lemma are prime. So the abstract algebra definition of “prime” is not the obvious generalization of the school mathematics definition. (To really work with “prime factorizations” in a ring like \( R \), we need to think about factoring subsets called ideals, rather than factoring elements. We’ll talk about ideals a bit later in the course, but probably won’t develop the theory of factoring them.)

(6) The last part of Chapter 5 connects our work with greatest common divisors to the usual late-elementary/middle school approach in terms of prime factorizations.