10.4: The Fundamental Theorem of Arithmetic

The **fundamental theorem of arithmetic** states that any integer greater than 1 has a unique prime factorization. For example, 12 factors into primes as \(12 = 2 \cdot 2 \cdot 3\), and moreover any factorization of 12 into primes uses exactly the primes 2, 2 and 3. Our proof combines the techniques of induction, cases, minimum counterexample and the idea of uniqueness of existence outlined at the end of Section 7.3.

**Theorem 10.1 (Fundamental Theorem of Arithmetic)**

Any integer \(n > 1\) has a unique prime factorization. “Unique” means that if \(n = p_{1} \cdot p_{2} \cdot p_{3} \cdots p_{k}\) and \(n = a_{1} \cdot a_{2} \cdot a_{3} \cdots a_{l}\) are two prime factorizations of \(n\), then \(k = l\), and the primes \(p_{i}\) and \(a_{i}\) are the same, except that they may be in different orders.

**Proof.** Suppose \(n > 1\). We first use strong induction to show that \(n\) has a prime factorization. For the basis step, if \(n = 2\), it is prime, so it is already its own prime factorization. Let \(n \geq 2\) and assume every integer between 2 and \(n\) (inclusive) has a prime factorization. Consider \(n + 1\). If it is prime, then it is its own prime factorization. If it is not prime, then it factors as \(n+1 = ab\) with \(a, b > 1\). Because \(a\) and \(b\) are both less than \(n+1\) they have prime factorizations \(a = p_{1} \cdot p_{2} \cdot p_{3} \cdots p_{k}\) and \(b = p_{1} \cdot p_{2} \cdot p_{3} \cdots p_{l}\). Then

\[
(n+1 = ab = (p_{1} \cdot p_{2} \cdot p_{3} \cdots p_{k}) (p'_{1} \cdot p'_{2} \cdot p'_{3} \cdots p'_{l}))
\]

is a prime factorization of \((n+1)\). This competes the proof by strong induction that every integer greater than 1 has a prime factorization.

Next we use proof by smallest counterexample to prove that the prime factorization of any \(n \geq 2\) is unique. If \(n = 2\), then \(n\) clearly has only one prime factorization, namely itself. Assume for the sake of contradiction that there is an \(n > 2\)
that has different prime factorizations \( n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k \) and \( n = a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_l \). Assume \( n \) is the smallest number with this property. From \( n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k \), we see that \( p_1 \mid n \), so \( p_1 \mid (a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_l) \). By Proposition 10.1 (page 186), \( p_1 \) divides one of the primes \( a_i \). As \( a_i \) is prime, we have \( p_1 = a_i \). Dividing \( n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k = a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_i \cdot \ldots \cdot a_l \) by \( p_1 = a_i \) yields

\[
\frac{n}{p_1} = \frac{p_2 \cdot p_3 \cdot \ldots \cdot p_k}{a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_i \cdot \ldots \cdot a_l}.
\]

These two factorizations are different, because the two prime factorizations of \( n \) were different. (Remember: the primes \( p_1 \) and \( a_i \) are equal, so the difference appears in the remaining factors, displayed above.) But also the above number \( \frac{p_2 \cdot \cdots \cdot p_k}{a_1 \cdot \cdots \cdot a_i \cdot \cdots \cdot a_l} \) is smaller than \( n \), and this contradicts the fact that \( n \) was the smallest number with two different prime factorizations.

A word of caution about induction and proof by smallest counterexample: In proofs in other textbooks or in mathematical papers, it often happens that the writer doesn’t tell you up front that these techniques are being used. Instead, you will have to read through the proof to glean from context what technique is being used. In fact, the same warning applies to all of our proof techniques. If you continue with mathematics, you will gradually gain through experience the ability to analyze a proof and understand exactly what approach is being used when it is not stated explicitly. Frustrations await you, but do not be discouraged by them. Frustration is a natural part of anything that’s worth doing.