In this handout, we discuss two results on prime numbers in Chapter 23 of Eccles.

Proposition 23.1.2. *Every integer greater than* 1 *can be written as the product of prime numbers.*

In other words, every integer ≥ 2 is either a prime or is the product of 2 or more primes.

For example, the first 9 such numbers are: 2, 3, $4 = 2 \cdot 2$, 5, $6 = 2 \cdot 3$, 7, $8 = 2 \cdot 2 \cdot 2$, $9 = 3 \cdot 3$, $10 = 2 \cdot 5$.

Proof of Proposition 23.1.2 (by strong induction). Recall that in strong induction we need to prove the base case and the following:

If $P(1), P(2), \ldots, P(k)$ are true for some $k \in \mathbb{Z}^+$, **then** $P(k+1)$ is true.

(1) Base case: 2 is a prime, so it is the product of a single prime.

(2) Strong inductive step: Suppose that for some $k \geq 2$ each integer n satisfying $2 \leq n \leq k$ may be written as a product of primes. We need to prove that $k+1$ is a product of primes.

Case (a): Suppose $k+1$ is a prime. Then we are done.

Case (b): Suppose $k+1$ is a not prime. Then there exist integers a, b with $2 \leq a, b \leq k$ such that

$$k + 1 = a \cdot b.$$

By the strong inductive hypothesis, both a and b are the product of primes. Thus $k+1 = a \cdot b$ is the product of primes.

(3) We are done by strong induction.

Theorem 23.5.1. *There are infinitely many primes.*

Proof (by contradiction). Suppose that the set of all primes is finite. Then we may write this set as

$$P = \{p_1, p_2, \ldots, p_n\},$$

where n is the cardinality of this set of all primes. By Proposition 23.1.2, for any integer $m > 1$ there exists i such that p_i divides m. On the other hand, for each i, p_i does not divide the integer

$$m = p_1 p_2 \cdots p_n + 1$$

since $m \equiv 1 \bmod p_i$ and $p_i > 1$. Since $m > 1$, we obtain a contradiction.

Remark. In other words, suppose p_i divides $p_1 p_2 \cdots p_n + 1$ for some $1 \leq i \leq n$. Since p_i divides $p_1 p_2 \cdots p_n$, this implies that p_i divides 1, a contradiction.