Theorem 2.8.2 *Let m, n be two positive integers and define*

$$S \equiv \{xm + yn \in \mathbb{N} : x, y \in \mathbb{Z}\}.$$

Then the smallest number in S is the greatest common divisor, denoted by (m, n).

Proof: First note that both m and n are in S so it is a nonempty set of positive integers. By well ordering, there is a smallest element of S, called $p = x_0 m + y_0 n$. Either p divides m or it does not. If p does not divide m, then by Theorem 2.7.11, $m = pq + r$ where $0 < r < p$. Thus $m = (x_0 m + y_0 n) q + r$ and so, solving for r,

$$r = m(1 - x_0) + (-y_0 q) n \in S.$$

However, this is a contradiction because p was the smallest element of S. Thus $p|m$. Similarly $p|n$.

Now suppose q divides both m and n. Then $m = qx$ and $n = qy$ for integers, x and y. Therefore,

$$p = mx_0 + ny_0 = x_0 qx + y_0 qy = q(x_0 x + y_0 y)$$

showing $q|p$. Therefore, $p = (m, n)$. ■

This amazing theorem will now be used to prove a fundamental property of prime numbers which leads to the fundamental theorem of arithmetic, the major theorem which says every integer can be factored as a product of primes.

Theorem 2.8.3 *If p is a prime and $p|ab$ then either $p|a$ or $p|b$.*

Proof: Suppose p does not divide a. Then since p is prime, the only factors of p are 1 and p so follows $(p, a) = 1$ and therefore, there exists integers, x and y such that $1 = ax + yp$. Multiplying this equation by b yields $b = abx + ybp$. Since $p|ab$, $ab = pz$ for some integer z. Therefore, $b = abx + ybp = pzx + ybp = p(xz + yb)$ and this shows p divides b. ■

Theorem 2.8.4 *(Fundamental theorem of arithmetic) Let $a \in \mathbb{N} \setminus \{1\}$. Then $a = \prod_{i=1}^{n} p_i$ where p_i are all prime numbers. Furthermore, this prime factorization is unique except for the order of the factors.*

Proof: If a equals a prime number, the prime factorization clearly exists. In particular the prime factorization exists for the prime number 2. Assume this theorem is true for all $a \leq n - 1$. If n is a prime, then it has a prime factorization. On the other hand, if n is not a prime, then there exist two integers k and m such that $n = km$ where each of k and m are less than n. Therefore, each of these is no larger than $n - 1$ and consequently, each has a prime factorization. Thus so does n. It remains to argue the prime factorization is unique except for order of the factors.

Suppose $\prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_j$ where the p_i and q_j are all prime, there is no way to reorder the q_k such that $m = n$ and $p_i = q_i$ for all i, and $n + m$ is the smallest positive integer such that this happens. Then by Theorem 2.8.3, $p_1 | q_j$ for some j. Since these are prime numbers this requires $p_1 = q_j$. Reordering if necessary it can be assumed that $q_j = q_1$. Then dividing both sides by $p_1 = q_1$, $\prod_{i=1}^{n-1} p_{i+1} = \prod_{j=1}^{m-1} q_{j+1}$. Since $n + m$ was as small as possible for the theorem to fail, it follows that $n - 1 = m - 1$ and the prime numbers, $q_2, \cdots, q_m$ can be reordered in such a way that $p_k = q_k$ for all $k = 2, \cdots, n$. Hence $p_i = q_i$ for all i because it was already argued that $p_1 = q_1$, and this results in a contradiction. ■