2.2 The Fundamental Theorem of Arithmetic

Theorem 2.2.1 (2.6 of text)**.** Let $a, b, n \in \mathbb{Z}$. If n and a are relatively prime and $n \mid (ab)$, then $n \mid b$.

Proof. Assume that n and a are relatively prime and $n \mid (ab)$. We shall prove that $n \mid b$. Since n and a are relatively prime, there are $x, y \in \mathbb{Z}$ such that $xn + ya = 1$ by Theorem 2.1.8. Now multiply both sides of this equation by b, obtaining $(xb)n + y(ab) = b$. Now since $n \mid n$ and (by assumption) $n \mid (ab)$, Theorem 1.2.4 implies that $n \mid b$. □

Theorem 2.2.2. Let a, b, n be integers where $a \mid n$ and $b \mid n$. If $(a, b) = 1$, then $(ab) \mid n$.

Proof. Assume that $(a, b) = 1$. We shall prove that $(ab) \mid n$. Because $a \mid n$, we have that $n = ak$ for some integer k. Since $b \mid n$ and $n = ak$, we have that $b \mid (ak)$. Now, because $(a, b) = 1$, Theorem 2.2.1 implies that $b \mid k$ and so, $k = b\ell$ for some integer ℓ. From $n = ak$ we now conclude that $n = (ab)\ell$. Thus, $(ab) \mid n$. □

Definition 2.2.3. Let $a, m, n \in \mathbb{Z}$. We write $(a, m, n) = d$ to denote the largest integer $d > 0$ that divides *all three* of the integers a, m, n.

Theorem 2.2.4 (2.7 of text)**.** Let $a, m, n \in \mathbb{Z}$ and suppose that $(a, m, n) = 1$. Then

$$(a, mn) = (a, m) \cdot (a, n).$$

Consequently, if $(a, m) = (a, n) = 1$, then $(a, mn) = 1$.

Proof. Let $d = (a, mn)$, $e = (a, m)$ and $f = (a, n)$. We shall prove that $d = ef$. Because $e = (a, m)$ and $f = (a, n)$, Theorem 2.1.6 implies there are integers w, x, y, z such that

$$wa + xm = e, \quad ya + zn = f.$$

Thus, $(wa + xm)(ya + zn) = ef$ and, after expanding, we obtain the equation

$$waya + wazn + xmya + xmzn = ef.$$

After "distributing out" a and separating mn, we obtain the equation

$$(way + wzn + xmy)a + (xz)(mn) = ef.$$

Since $d = (a, mn)$, Theorem 1.2.4 implies that $d \mid (ef)$ and therefore, $d \leq ef$.

We will now show that $ef \leq d$. Since $e = (a, m)$, $f = (a, n)$ and $(a, m, n) = 1$, we see that $(e, f) = 1$. Furthermore, because $d = (a, mn)$, Theorem 2.1.6 asserts there are integers i and j such that $(*)$ $ia + j(mn) = d$. Since $e = (a, m)$, equation $(*)$ and Theorem 1.2.4 imply that $e \mid d$. Similarly, since $f = (a, n)$, we see that $f \mid d$. Now, because $e \mid d$, $f \mid d$ and $(e, f) = 1$, Theorem 2.2.2 implies that $(ef) \mid d$. Therefore, $ef \leq d$. We can now deduce that $d = ef$. □

Theorem 2.2.5. Let $a, b \in \mathbb{Z}$. Let p be a prime number. If $p \mid (ab)$, then $p \mid a$ or $p \mid b$.

Proof. Let $a, b \in \mathbb{Z}$. Assume that p is a prime. We shall prove that if $p \mid (ab)$, then $p \mid a$ or $p \mid b$. So assume that $p \mid (ab)$. We shall prove that $p \mid a$ or $p \mid b$. So, assume that $p \nmid a$. We shall prove that $p \mid b$. Since $p \nmid a$ and p is a prime, it follows that $(a, p) = 1$. Theorem 2.2.1 implies that $p \mid b$. This completes the proof. $\square$

One can prove the following theorem by induction on n, using Theorem 2.2.5.

Theorem 2.2.6 (2.8 of text)**.** Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Let p be a prime number. If $p \mid (a_1 a_2 \cdots a_n)$, then $p \mid a_i$ for some i with $1 \leq i \leq n$. As a special case, if $p \mid a^n$, then $p \mid a$.

Proof. We prove, by mathematical induction, that for all $n \geq 2$ if $p \mid (a_1 a_2 \cdots a_n)$, then $p \mid a_i$ for some i with $1 \leq i \leq n$.

Base step: For $n = 2$, assume that $p \mid (a_1 a_2)$. Theorem 2.2.5 implies that either $p \mid a_1$ or $p \mid a_2$.

Inductive step: Let $n \geq 2$ be arbitrary and assume the induction hypothesis

$$\text{if } p \mid (a_1 a_2 \cdots a_n), \text{ then } p \mid a_i \text{ for some } i \text{ with } 1 \leq i \leq n. \tag{IH}$$

We show that if $p \mid (a_1 a_2 \cdots a_n a_{n+1})$, then $p \mid a_i$ for some i with $1 \leq i \leq n+1$. Assume that $p \mid (a_1 a_2 \cdots a_n a_{n+1})$. Thus, $p \mid (a_1 a_2 \cdots a_n) a_{n+1}$. Theorem 2.2.5 implies that either $p \mid (a_1 a_2 \cdots a_n)$ or $p \mid a_{n+1}$. If $p \mid (a_1 a_2 \cdots a_n)$, then the induction hypothesis (IH) implies that $p \mid a_i$ for some i with $1 \leq i \leq n$. Thus, in either case, we can conclude that $p \mid a_i$ for some i with $1 \leq i \leq n+1$ and the proof is complete. $\square$

Theorem 2.2.7 (Existence of Prime Factorization)**.** Let $n > 1$ be a natural number. Then n can be expressed as a finite product of primes, that is, there are prime numbers $p_1, p_2, \ldots, p_k$ with $k \geq 1$ such that $n = p_1 p_2 \cdots p_k$.

Proof. Suppose, for a contradiction, that there are natural numbers that cannot be expressed as a product of primes. By the Well-Ordering Principle, there is a smallest such natural number. Let N be this smallest natural number. Thus, if $1 < n < N$, then n can be expressed as a product of primes. By Theorem 1.2.7, N is divisible by some prime p. Note that $N \neq p$, because $N = p$ expresses N as a product of primes. Thus, $N = n \cdot p$ where $1 < n < N$. Since $1 < n < N$, it follows that $n = p_1 p_2 \cdots p_k$ for some prime numbers $p_1, p_2, \ldots, p_k$ with $k \geq 1$. Therefore, $N = np = p_1 p_2 \cdots p_k p$ can be written as a finite product of primes. This contradiction shows that the theorem is true for all natural numbers greater than 1. $\square$

Definition 2.2.8. Let $n > 1$ be a natural number. We shall say that a prime factorization $n = p_1 p_2 \cdots p_k$ is in *ascending order* if $p_i \leq p_j$ when $1 \leq i \leq j \leq k$. We shall also call such a prime factorization an *ascending* prime factorization.

Example 1. Ascending prime factorizations: $10 = 2 \cdot 5$, $20 = 2 \cdot 2 \cdot 5$, $13 = 13$, $84 = 2 \cdot 3 \cdot 3 \cdot 7$.

Theorem 2.2.9 (2.9 of text)**.** Let $n > 1$ be a natural number. Suppose that $n = p_1 p_2 \cdots p_r$ is an ascending prime factorization and that $n = q_1 q_2 \cdots q_s$ is also an ascending prime factorization. Then $r = s$ and $p_1 = q_1, p_2 = q_2, \ldots, p_r = q_s$.

Proof. Suppose, for a contradiction, that there are natural numbers with two different ascending prime factorizations. By the Well-Ordering Principle, there is a smallest such natural number. Let N be this smallest natural number. Thus, if $1 < n < N$, then n can be expressed as an ascending product of primes in exactly one way. Now, let $N = p_1 p_2 \cdots p_r$ and $N = q_1 q_2 \cdots q_s$ be two different ascending prime factorizations. There are three separate cases to consider: Either (1) $q_s < p_r$, (2) $p_r < q_s$ or (3) $p_r = q_s$.

CASE (1): Suppose that $q_s < p_r$. Since $N = p_1 p_2 \cdots p_r$, it follows that $p_r \mid N$. Moreover, because $N = q_1 q_2 \cdots q_s$, it follows that $p_r \mid (q_1 q_2 \cdots q_s)$. By Theorem 2.2.6, there is an i with $1 \le i \le s$ such that $p_r \mid q_i$. Since p_r and q_i are both primes, it follows that $p_r = q_i$. However, $q_i \le q_s$ and $q_s < p_r$. Hence, $q_i \le q_s < p_r = q_i$ and thus, $q_i < q_i$ which is impossible. Therefore, we cannot have that $q_s < p_r$.

CASE (2): Suppose that $p_r < q_s$. An argument similar to the one given in Case (1) will show that $p_r < q_s$ is impossible.

CASE (3): Suppose that $p_r = q_s$. To simplify notation, let $\overline{p} = p_r = q_s$. Observe that $N \ne \overline{p}$. Because, if $N = \overline{p}$ then N is a prime and we must conclude that $r = s = 1$ with $p_1 = q_1$. Thus, the ascending prime factorizations for N are exactly the same. Therefore, $N \ne \overline{p}$ and so, $r \ge 2$ and $s \ge 2$. Thus, we can write $N = p_1 p_2 \cdots p_{r-1} p_r = p_1 p_2 \cdots p_{r-1}\overline{p}$ and $N = q_1 q_2 \cdots q_{s-1} q_s = q_1 q_2 \cdots q_{s-1}\overline{p}$. Therefore,

$$p_1 p_2 \cdots p_{r-1}\overline{p} = q_1 q_2 \cdots q_{s-1}\overline{p}.$$

By cancelling $\overline{p}$, we conclude that $n = p_1 p_2 \cdots p_{r-1} = q_1 q_2 \cdots q_{s-1}$ with $1 < n < N$. Since $1 < n < N$, it follows that $r - 1 = s - 1$ and $p_1 = q_1$, $p_2 = q_2$, $\ldots$, $p_{r-1} = q_{s-1}$. Thus, $r = s$ and since $p_r = q_s$, we conclude that the ascending prime factorizations $N = p_1 p_2 \cdots p_r$ and $N = q_1 q_2 \cdots q_s$ are exactly the same. This contradiction shows that the theorem is true for all natural numbers greater than 1. □

Example 2. Simplifying ascending prime factorizations: $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$, $56 = 2 \cdot 2 \cdot 2 \cdot 7 = 2^3 \cdot 7$, $882 = 2 \cdot 3 \cdot 3 \cdot 7 \cdot 7 = 2 \cdot 3^2 \cdot 7^2$, $6936 = 2^3 \cdot 3 \cdot 17^2$, $1200 = 2^4 \cdot 3 \cdot 5^2$.

It often happens that certain primes occur more that once in a prime factorization of a composite natural number. In this case we shall simplify the prime factorization by using exponents, as in the above example, and write

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

where p_1, p_2, $\ldots$ p_k are distinct primes and $a_1 \ge 1, a_2 \ge 1, \ldots, a_k \ge 1$.

Theorem 2.2.10 (Fundamental Theorem of Arithmetic)**.** Let $n > 1$ be a natural number. Then there exists distinct primes $p_1, p_2, \ldots, p_n$ and exponents $a_1 \ge 1, a_2 \ge 1, \ldots, a_k \ge 1$ such that

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}.$$

Furthermore, given any prime factorization into distinct primes

$$n = q_1^{b_1} q_2^{b_2} \cdots q_\ell^{b_\ell}$$

then $\ell = k$, the primes q_i are the same as the primes p_j (except for order) and the corresponding exponents are the same.

Note that if p, q are primes and $p \mid q$, then $p = q$. The following theorem now follows directly from Theorem 2.2.6.

Theorem 2.2.11 (2.10 of text)**.** Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ be the prime factorization of $n > 1$. Let p be a prime number. If $p \mid n$, then $p = p_i$ for some i with $1 \leq i \leq k$.

Another way to get the greatest common divisor

Lemma 2.2.12. Let a and b be two natural numbers greater than 1 with prime factorizations $a = q_1 q_2 \cdots q_i$ and $b = r_1 r_2 \cdots r_j$ where none of the q's are equal to any of the r's. Then $(a, b) = 1$. Thus for $k \geq 1$, if $k \mid a$ and $k \mid b$, then $k = 1$.

Proof. Let $d = (a, b)$. Suppose, for a contradiction, that $d > 1$. Since $d > 1$, Theorem 1.2.7 implies that $p \mid d$ for some prime p. We know that $d \mid a$ and $d \mid b$. Because $p \mid d$, Theorem 1.2.5 implies that $p \mid a$ and $p \mid b$. Because $p \mid (q_1 q_2 \cdots q_i)$, Theorem 2.2.11 implies that $p = q_k$ for some k with $1 \leq k \leq i$. Furthermore, because $p \mid (r_1 r_2 \cdots r_j)$, Theorem 2.2.11 also implies that $p = r_\ell$ for some ℓ with $1 \leq \ell \leq j$. Therefore, $p = q_k = r_\ell$. This contradicts the assumption that no prime q is equal to any prime r. Therefore, we must have that $d = 1$. Since $(a, b) = 1$, we clearly have for $k \geq 1$ if $k \mid a$ and $k \mid b$, then $k = 1$ by Theorem 2.1.7. □

Theorem 2.2.13 (2.11 of text)**.** Let n and m be two natural numbers greater than 1 with prime factorizations

$$\begin{aligned} n &= p_1 p_2 \cdots p_k q_1 q_2 \cdots q_i \\ m &= p_1 p_2 \cdots p_k r_1 r_2 \cdots r_j \end{aligned}$$

where none of the q's are equal to any of the r's. Then $(n, m) = p_1 p_2 \cdots p_k$.

In the statement of the above theorem, we are allowing for the possibility that $k = 0$ and, in this case, $p_1 p_2 \cdots p_k = 1$. Similarly, we are also allowing for the possibility that $i = 0$ and $j = 0$. We now prove this theorem.

Proof. Let $d = (n, m)$ and let $e = p_1 p_2 \cdots p_k$. We shall prove that $d = e$. Thus $n = e(q_1 q_2 \cdots q_i)$ and $m = e(r_1 r_2 \cdots r_j)$. Clearly, $e \mid n$ and $e \mid m$. Therefore, $e \mid d$ by Theorem 2.1.7. Therefore, $d = ek$ for some natural number k. We know that $d \mid a$ and $d \mid b$. So, $ek \mid e(q_1 q_2 \cdots q_i)$ and $ek \mid e(r_1 r_2 \cdots r_j)$. Theorem 1.2.6 implies that $k \mid (q_1 q_2 \cdots q_i)$ and $k \mid (r_1 r_2 \cdots r_j)$. Lemma 2.2.12 implies that $k = 1$. Therefore, $d = e$. □

Example 3. Find (a, b) for the following:

1. $a = 100 = 2^2 \cdot 5^2$, $b = 56 = 2^3 \cdot 7$;
2. $a = 882 = 2 \cdot 3^2 \cdot 7^2$, $b = 168 = 2^2 \cdot 3 \cdot 7$;
3. $6936 = 2^3 \cdot 3 \cdot 17^2$, $b = 1200 = 2^4 \cdot 3 \cdot 5^2$.

Exercises 2.2

Do problems #$\boxed{1}$, 3, 5, 6, 7, $\boxed{12}$, 15, on pages 32-33 of text.

Exercise Notes. Problem 7: for positive p and n, if $p \mid n$ and $p \neq n$, then $n = ap$ for some $a \geq 2$. So, $n \geq 2p$. Problem 15: use a prime factorization with 4 distinct primes.

Do only squared problems