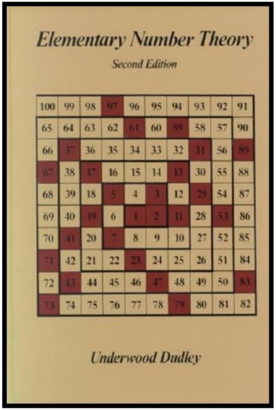
Elementary Number Theory

Section 2. Unique Factorization—Proofs of Theorems



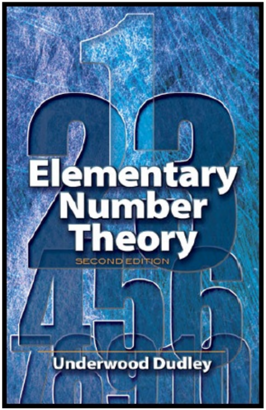


Table of contents

Lemma 2.1

Lemma 2.1. Every integer n, with $n > 1$, is divisible by a prime.

Proof. Consider the set D of divisors of n which are greater than 1 and less than n. First, if D is empty then n is prime by definition and since it divides itself then n has a prime divisor.

Second, if D is nonempty, then the Least-Integer Principle implies that D has a least element d. If d had a divisor a greater than 1 and less than d, then a would also be a divisor of n (by the definition of divisiblity). But since d is the least such divisor of n, then no such a exists and hence d is prime. That is, d is a prime divisor of n.

So in both cases (namely, $D = \varnothing$ and $D \neq \varnothing$) we have a prime divisor of n and the claim follows. $\square$

Lemma 2.1

Lemma 2.1. Every integer n, with $n > 1$, is divisible by a prime.

Proof. Consider the set D of divisors of n which are greater than 1 and less than n. First, if D is empty then n is prime by definition and since it divides itself then n has a prime divisor.

Second, if D is nonempty, then the Least-Integer Principle implies that D has a least element d. If d had a divisor a greater than 1 and less than d, then a would also be a divisor of n (by the definition of divisiblity). But since d is the least such divisor of n, then no such a exists and hence d is prime. That is, d is a prime divisor of n.

So in both cases (namely, $D = \varnothing$ and $D \neq \varnothing$) we have a prime divisor of n and the claim follows. □

Lemma 2.2

Lemma 2.2. Every integer n, with $n > 1$, can be written as a product of primes.

Proof. By Lemma 2.1, there is a prime p_1 such that $p_1 \mid n$. That is, $n = p_1 n$ where $1 \leq n_1 < n$. If $n_1 = 1$ then $n = p_1$ and we are done. If $n_1 > 1$ then from Lemma 2.1 again there is a prime p_2 that divides n_1. That is, $n_1 = p_2 n_2$ where p_2 is prime and $1 \leq n_2 < n_1$. If $n_2 = 1$ then $n = p_1 p_2$ and we are done. If $n_2 > 1$ then, similarly, by Lemma 2.1 we have $n_2 = p_3 n_3$ with p_3 prime and $1 \leq n_3 < n_2$. If $n_3 = 1$ then $n = p_1 p_2 p_3$ and we are done. Continuing we produce $n > n_1 > n_2 > n_3 > \cdots$ and each n_1 is positive, so the must end at some $n_k = 1$ in which case $n = p_1 p_2 \cdots p_k$; that is, n is a product of primes. $\square$

Lemma 2.2

Lemma 2.2. Every integer n, with $n > 1$, can be written as a product of primes.

Proof. By Lemma 2.1, there is a prime p_1 such that $p_1 \mid n$. That is, $n = p_1 n$ where $1 \leq n_1 < n$. If $n_1 = 1$ then $n = p_1$ and we are done. If $n_1 > 1$ then from Lemma 2.1 again there is a prime p_2 that divides n_1. That is, $n_1 = p_2 n_2$ where p_2 is prime and $1 \leq n_2 < n_1$. If $n_2 = 1$ then $n = p_1 p_2$ and we are done. If $n_2 > 1$ then, similarly, by Lemma 2.1 we have $n_2 = p_3 n_3$ with p_3 prime and $1 \leq n_3 < n_2$. If $n_3 = 1$ then $n = p_1 p_2 p_3$ and we are done. Continuing we produce $n > n_1 > n_2 > n_3 > \cdots$ and each n_1 is positive, so the must end at some $n_k = 1$ in which case $n = p_1 p_2 \cdots p_k$; that is, n is a product of primes. $\square$

Theorem 2.1

Theorem 2.1. Euclid's Theorem.
There are infinitely many primes.

Proof. We give a proof by contradiction. ASSUME there are only finitely many primes, say $p_1, p_2, \ldots, p_r$. Consider the integer $n = p_1 p_2 \cdots p_r + 1$. By Lemma 2.1, n is divisible by a prime and since we have assumed there are only finitely many primes, the divisor must be one of $p_1, p_2, \ldots, p_r$. Suppose that it is p_k.

Theorem 2.1

Theorem 2.1. Euclid's Theorem.
There are infinitely many primes.

Proof. We give a proof by contradiction. ASSUME there are only finitely many primes, say $p_1, p_2, \ldots, p_r$. Consider the integer $n = p_1 p_2 \cdots p_r + 1$. By Lemma 2.1, n is divisible by a prime and since we have assumed there are only finitely many primes, the divisor must be one of $p_1, p_2, \ldots, p_r$. Suppose that it is p_k.

Then we have $p_k \mid n$ and $p \mid p_1 p_2 \cdots p_r$ and so, by Lemma 1.2, $p_k \mid (n - p_1 p_2 \cdots p_r)$ or, in other words, $p_k \mid 1$. But this is a CONTRADICTION since no prime divides 1. So the assumption that there are finitely many primes must be false and hence there are infinitely many primes, as claimed. $\square$

Theorem 2.1

Theorem 2.1. Euclid's Theorem.
There are infinitely many primes.

Proof. We give a proof by contradiction. ASSUME there are only finitely many primes, say $p_1, p_2, \ldots, p_r$. Consider the integer $n = p_1 p_2 \cdots p_r + 1$. By Lemma 2.1, n is divisible by a prime and since we have assumed there are only finitely many primes, the divisor must be one of $p_1, p_2, \ldots, p_r$. Suppose that it is p_k.

Then we have $p_k \mid n$ and $p \mid p_1 p_2 \cdots p_r$ and so, by Lemma 1.2, $p_k \mid (n - p_1 p_2 \cdots p_r)$ or, in other words, $p_k \mid 1$. But this is a CONTRADICTION since no prime divides 1. So the assumption that there are finitely many primes must be false and hence there are infinitely many primes, as claimed. $\square$

Lemma 2.3

Lemma 2.3. If n is composite, then it has a divisor d such that $1 < d \leq n^{1/2}$.

Proof. Since n is composite, then there are integers d_1 and d_2 such that $d_1 d_2 = n$, $1 < d_1 < n$, and $1 < d_2 < n$. If $d_1 > n1/2$ and $d_2 > n^{1/2}$ then $n = d_1 d_2 > n^{1/2} n^{1/2} = n$, a contradictions. So one of d_1 or d_2 must be less than or equal to $n^{1/2}$, as claimed. □

Lemma 2.3

Lemma 2.3. If n is composite, then it has a divisor d such that $1 < d \leq n^{1/2}$.

Proof. Since n is composite, then there are integers d_1 and d_2 such that $d_1 d_2 = n$, $1 < d_1 < n$, and $1 < d_2 < n$. If $d_1 > n1/2$ and $d_2 > n^{1/2}$ then $n = d_1 d_2 > n^{1/2} n^{1/2} = n$, a contradictions. So one of d_1 or d_2 must be less than or equal to $n^{1/2}$, as claimed. $\square$

Lemma 2.4

Lemma 2.4. If n is composite, then it has a *prime* divisor d such that $1 < d \leq n^{1/2}$.

Proof. By Lemma 2.3, n has a divisor d such that $1 < d \leq n^{1/2}$. By Lemma 2.1, d has a prime divisor p. So $1 < p \leq d \leq n^{1/2}$ and the claim holds. □

Lemma 2.4

Lemma 2.4. If n is composite, then it has a *prime* divisor d such that $1 < d \leq n^{1/2}$.

Proof. By Lemma 2.3, n has a divisor d such that $1 < d \leq n^{1/2}$. By Lemma 2.1, d has a prime divisor p. So $1 < p \leq d \leq n^{1/2}$ and the claim holds. □

Lemma 2.5

Lemma 2.5. Euclid's Lemma.
For p prime, if $p \mid ab$ then either $p \mid a$ or $p \mid b$.

Proof. Since p is prime, its only positive divisors are 1 and p. So the greatest common divisor (p, a) must be either 1 or p; that is, either $(p, a) = 1$ or $(p, a) = p$. If $(p, a) = p$ then $p \mid a$ and we are done. If $(p, a) = 1$ then, since $p \mid ab$ by hypothesis, by Corollary 1.1 we have $p \mid b$. So either $p \mid a$ or $p \mid b$, as claimed. $\square$

Lemma 2.5

Lemma 2.5. Euclid's Lemma.
For p prime, if $p \mid ab$ then either $p \mid a$ or $p \mid b$.

Proof. Since p is prime, its only positive divisors are 1 and p. So the greatest common divisor (p, a) must be either 1 or p; that is, either $(p, a) = 1$ or $(p, a) = p$. If $(p, a) = p$ then $p \mid a$ and we are done. If $(p, a) = 1$ then, since $p \mid ab$ by hypothesis, by Corollary 1.1 we have $p \mid b$. So either $p \mid a$ or $p \mid b$, as claimed. $\square$

Lemma 2.6

Lemma 2.6. For p prime, if $p \mid (a_1 a_2 \cdots a_k)$ then $p \mid a_i$ for some $i = 1, 2, \ldots, k$.

Proof. If $k = 1$ then the result holds trivially. If $k = 2$ the the result holds by Lemma 2.5. We now give a proof using Mathematical Induction with $k = 1$ and $k = 2$ as Base Cases. Suppose the claim holds for $k = r$; that is, suppose $p \mid (a_1 a_2 \cdots a_r)$ implies $p \mid a_i$ for some $i = 1, 2, \ldots, r$ (this is the Induction Hypothesis).

Lemma 2.6

Lemma 2.6. For p prime, if $p \mid (a_1 a_2 \cdots a_k)$ then $p \mid a_i$ for some $i = 1, 2, \ldots, k$.

Proof. If $k = 1$ then the result holds trivially. If $k = 2$ the the result holds by Lemma 2.5. We now give a proof using Mathematical Induction with $k = 1$ and $k = 2$ as Base Cases. Suppose the claim holds for $k = r$; that is, suppose $p \mid (a_1 a_2 \cdots a_r)$ implies $p \mid a_i$ for some $i = 1, 2, \ldots, r$ (this is the Induction Hypothesis).

Next, suppose that $p \mid (a_1 a_2 \cdots a_{r+1})$. Then $p \mid (a_1 a_2 \cdots a_r) a_{r+1}$ and by Lemma 2.5 we have that either $p \mid (a_1 a_2 \cdots a_r)$ or $p \mid a_{r+1}$. If $p \mid (a_1 a_2 \cdots a_r)$ then by the Induction Hypothesis we have that $p \mid a_i$ for some $i = 1, 2, \ldots, r$. If $p \mid a_{r+1}$ then we have $p \mid a_i$ for $i = r + 1$. Since one of these must be the case, then we have $p \mid a_i$ for some $i = 1, 2, \ldots, r, r + 1$. That is, the claim holds for $k = r + 1$. So by Mathematical Induction, the result holds for all positive integers k, as claimed. □

Lemma 2.6

Lemma 2.6. For p prime, if $p \mid (a_1 a_2 \cdots a_k)$ then $p \mid a_i$ for some $i = 1, 2, \ldots, k$.

Proof. If $k = 1$ then the result holds trivially. If $k = 2$ the the result holds by Lemma 2.5. We now give a proof using Mathematical Induction with $k = 1$ and $k = 2$ as Base Cases. Suppose the claim holds for $k = r$; that is, suppose $p \mid (a_1 a_2 \cdots a_r)$ implies $p \mid a_i$ for some $i = 1, 2, \ldots, r$ (this is the Induction Hypothesis).

Next, suppose that $p \mid (a_1 a_2 \cdots a_{r+1})$. Then $p \mid (a_1 a_2 \cdots a_r) a_{r+1}$ and by Lemma 2.5 we have that either $p \mid (a_1 a_2 \cdots a_r)$ or $p \mid a_{r+1}$. If $p \mid (a_1 a_2 \cdots a_r)$ then by the Induction Hypothesis we have that $p \mid a_i$ for some $i = 1, 2, \ldots, r$. If $p \mid a_{r+1}$ then we have $p \mid a_i$ for $i = r + 1$. Since one of these must be the case, then we have $p \mid a_i$ for some $i = 1, 2, \ldots, r, r + 1$. That is, the claim holds for $k = r + 1$. So by Mathematical Induction, the result holds for all positive integers k, as claimed. $\square$

Lemma 2.7

Lemma 2.7. If $q_1, q_2, \ldots, q_n$ are primes and $p \mid (q_1 q_2 \cdots q_n)$ then $p = q_k$ for some $k = 1, 2, \ldots, n$.

Proof. Since $p \mid (q_1 q_2 \cdots q_n)$, then by Lemma 2.6 we have that $p \mid q_k$ for some $k = 1, 2, \ldots, n$. Since q_k is prime then the only positive divisors of q_k are 1 and q_k itself. Since p is prime then it is not 1, so it must be that $p = q_k$ as claimed. $\square$

Lemma 2.7

Lemma 2.7. If $q_1, q_2, \ldots, q_n$ are primes and $p \mid (q_1 q_2 \cdots q_n)$ then $p = q_k$ for some $k = 1, 2, \ldots, n$.

Proof. Since $p \,|(q_1 q_2 \cdots q_n)$, then by Lemma 2.6 we have that $p \mid q_k$ for some $k = 1, 2, \ldots, n$. Since q_k is prime then the only positive divisors of q_k are 1 and q_k itself. Since p is prime then it is not 1, so it must be that $p = q_k$ as claimed. □

Theorem 2.2

Theorem 2.2. The Unique Factorization Theorem or **The Fundamental Theorem of Arithmetic.**
Any positive integer greater than 1 can be written as a product of primes in one and only one way.

Proof. First, we comment on what we mean by "unique." Two factorizations of a positive integer are considered the same if they involve the exact same factors, but the factors may appear in any order (because of the commutivity of multiplication).

Theorem 2.2

Theorem 2.2. The Unique Factorization Theorem or **The Fundamental Theorem of Arithmetic.**
Any positive integer greater than 1 can be written as a product of primes in one and only one way.

Proof. First, we comment on what we mean by "unique." Two factorizations of a positive integer are considered the same if they involve the exact same factors, but the factors may appear in any order (because of the commutivity of multiplication).

Let n be an integer greater than 1. By Lemma 2.2, n can be written as a product of primes. We just need to show that this product is unique in the sense described above. Consider two factorizations of n into products of primes:

$$n = p_1 p_2 \cdots p_m \text{ and } n = q_1 q_2 \cdots q_r,$$

where each p_i is prime for $i = 1, 2, \ldots, m$ and each q_i is prime for $i = 1, 2, \ldots, r$.

Theorem 2.2

Theorem 2.2. The Unique Factorization Theorem or **The Fundamental Theorem of Arithmetic.**
Any positive integer greater than 1 can be written as a product of primes in one and only one way.

Proof. First, we comment on what we mean by "unique." Two factorizations of a positive integer are considered the same if they involve the exact same factors, but the factors may appear in any order (because of the commutivity of multiplication).

Let n be an integer greater than 1. By Lemma 2.2, n can be written as a product of primes. We just need to show that this product is unique in the sense described above. Consider two factorizations of n into products of primes:

$$n = p_1 p_2 \cdots p_m \text{ and } n = q_1 q_2 \cdots q_r,$$

where each p_i is prime for $i = 1, 2, \ldots, m$ and each q_i is prime for $i = 1, 2, \ldots, r$.

Theorem 2.2 (continued 1)

Theorem 2.2. The Unique Factorization Theorem or **The Fundamental Theorem of Arithmetic.**
Any positive integer greater than 1 can be written as a product of primes in one and only one way.

Proof. We want to show that the same primes appear in each product and appear the same number of times; that is, we want to show that the integers $p_1, p_2, \ldots, p_m$ is a rearrangement of the integers $q_1, q_2, \ldots, q_r$ (notice that we will also need to show $m = r$).

Since $p_1 \mid n$ then $p_1 \mid (q_1 q_2 \cdots q_r)$. Lemma 2.7 then implies that $p_1 = q_i$ for some $i = 1, 2, \ldots, r$. Then dividing out $p_1 = q_i$ in the equation $p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_r$ we get $p_2 p_3 \cdots p_m = q_1 q_2 \cdots q_{i-1} q_{i+1} q_{i+2} \cdots q_r$. Similarly, p_2 divides $p_2 p_3 \cdots p_m = q_1 q_2 \cdots q_{i-1} q_{i+1} q_{i+2} \cdots q_r$ and again by Lema 2.7 we have $p_2 = q_j$ for some $j = 1, 2, \ldots, i-1, i+1, i+2, \ldots, r$.

Theorem 2.2 (continued 1)

Theorem 2.2. The Unique Factorization Theorem or **The Fundamental Theorem of Arithmetic.**
Any positive integer greater than 1 can be written as a product of primes in one and only one way.

Proof. We want to show that the same primes appear in each product and appear the same number of times; that is, we want to show that the integers $p_1, p_2, \ldots, p_m$ is a rearrangement of the integers $q_1, q_2, \ldots, q_r$ (notice that we will also need to show $m = r$).

Since $p_1 \mid n$ then $p_1 \mid (q_1 q_2 \cdots q_r)$. Lemma 2.7 then implies that $p_1 = q_i$ for some $i = 1, 2, \ldots, r$. Then dividing out $p_1 = q_i$ in the equation $p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_r$ we get $p_2 p_3 \cdots p_m = q_1 q_2 \cdots q_{i-1} q_{i+1} q_{i+2} \cdots q_r$. Similarly, p_2 divides $p_2 p_3 \cdots p_m = q_1 q_2 \cdots q_{i-1} q_{i+1} q_{i+2} \cdots q_r$ and again by Lema 2.7 we have $p_2 = q_j$ for some $j = 1, 2, \ldots, i-1, i+1, i+2, \ldots, r$.

Theorem 2.2 (continued 2)

Theorem 2.2. The Unique Factorization Theorem or **The Fundamental Theorem of Arithmetic.**
Any positive integer greater than 1 can be written as a product of primes in one and only one way.

Proof. Dividing out the common factor gives

$$p_3 p_4 \cdots p_m = q_1 q_2 \cdots q_{i-1} q_{i+1} q_{i+2} \cdots q_{j-1} q_{j+1} q_{j+2} \cdots q_r$$

(where, for the sake of illustration, we take $i < j$). We continue this process of dividing out prime factors. We cannot run out of q's before all the p's are gone since this would give an equality between 1 and a product of primes, which cannot happen. Similarly, we cannot divide out all the p's before all the q's are gone. That is, we must have the same number of p's and q's; in other words, $m = r$. So the p_i's can be rearranged to give (correspondingly) the q_j's. Hence the prime factors in $p_1 p_2 \cdots p_m$ and the prime factors in $q_1 q_2 \cdots q_r$ are exactly the same. That is, the prime factorization of n is unique, as claimed. □

Theorem 2.2 (continued 2)

Theorem 2.2. The Unique Factorization Theorem or **The Fundamental Theorem of Arithmetic.**
Any positive integer greater than 1 can be written as a product of primes in one and only one way.

Proof. Dividing out the common factor gives

$$p_3 p_4 \cdots p_m = q_1 q_2 \cdots q_{i-1} q_{i+1} q_{i+2} \cdots q_{j-1} q_{j+1} q_{j+2} \cdots q_r$$

(where, for the sake of illustration, we take $i < j$). We continue this process of dividing out prime factors. We cannot run out of q's before all the p's are gone since this would give an equality between 1 and a product of primes, which cannot happen. Similarly, we cannot divide out all the p's before all the q's are gone. That is, we must have the same number of p's and q's; in other words, $m = r$. So the p_i's can be rearranged to give (correspondingly) the q_j's. Hence the prime factors in $p_1 p_2 \cdots p_m$ and the prime factors in $q_1 q_2 \cdots q_r$ are exactly the same. That is, the prime factorization of n is unique, as claimed. □