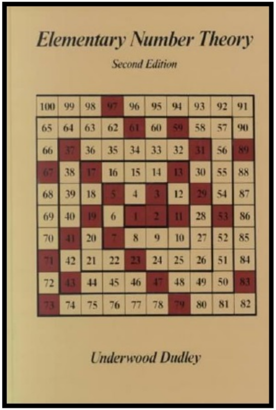
Elementary Number Theory

Section 7. The Divisors of an Integer—Proofs of Theorems



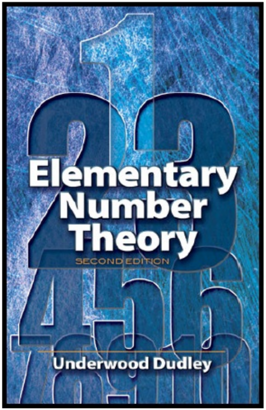


Table of contents

Theorem 7.1

Theorem 7.1. If $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime-power decomposition of n, then $d(n) = d(p_1^{e_1}) d(p_2^{e_2}) \cdots d(p_k^{e_k})$.

Proof. Let D denote the set of numbers $\{p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k} \mid 0 \leq f_i \leq e_i\}$. First, notice that every number in set D is a divisor of n, since

$$n = (p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k})(p_1^{e_1 - f_1} p_2^{e_2 - f_2} \cdots p_k^{e_k - f_k}).$$

Theorem 7.1

Theorem 7.1. If $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime-power decomposition of n, then $d(n) = d(p_1^{e_1}) d(p_2^{e_2}) \cdots d(p_k^{e_k})$.

Proof. Let D denote the set of numbers $\{p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k} \mid 0 \leq f_i \leq e_i\}$. First, notice that every number in set D is a divisor of n, since

$$n = (p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k})(p_1^{e_1 - f_1} p_2^{e_2 - f_2} \cdots p_k^{e_k - f_k}).$$

Second, suppose that d is a divisor of n. If $p^f \quad d$ then $p^f \mid n$, so each power of a prime in the prime-power decomposition of d must appear in the prime-power decomposition of n. Thus $d = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$ where each f_i is nonnegative. Moreover, no exponent f_i can be larger than e_i, for $p_i^{f_i} \mid d$ implies $p_i^{f_i} \mid n$ and this is not the case for $f_i > e_i$. That is, every divisor of n is an element of set D and so D is exactly the set of divisors of n. So the number of divisors of n is the number of elements of D.

Theorem 7.1

Theorem 7.1. If $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime-power decomposition of n, then $d(n) = d(p_1^{e_1}) d(p_2^{e_2}) \cdots d(p_k^{e_k})$.

Proof. Let D denote the set of numbers $\{p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k} \mid 0 \le f_i \le e_i\}$. First, notice that every number in set D is a divisor of n, since

$$n = (p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k})(p_1^{e_1 - f_1} p_2^{e_2 - f_2} \cdots p_k^{e_k - f_k}).$$

Second, suppose that d is a divisor of n. If $p^f \quad d$ then $p^f \mid n$, so each power of a prime in the prime-power decomposition of d must appear in the prime-power decomposition of n. Thus $d = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$ where each f_i is nonnegative. Moreover, no exponent f_i can be larger than e_i, for $p_i^{f_i} \mid d$ implies $p_i^{f_i} \mid n$ and this is not the case for $f_i > e_i$. That is, every divisor of n is an element of set D and so D is exactly the set of divisors of n. So the number of divisors of n is the number of elements of D.

Theorem 7.1 (continued)

Proof (continued). With $D = \{p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k} \mid 0 \leq f_i \leq e_i\}$, we see that each f_i may take on $e_1 + 1$ different values. Thus, there are $(e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$ numbers in D and, by the Unique Factorization Theorem (Theorem 2.2, the Fundamental Theorem of Arithmetic), they are all different. (In this claim, we are using the Fundamental Principle of Counting also. See my online notes for Foundations of Probability and Statistics-Calculus Based (MATH 2050) on Section 2.2. Counting Methods [notice Note 2.2.A], my notes for Applied Combinatorics and Problem Solving [MATH 3340] on Section 1.1. The Fundamental Counting Principle, or my notes for Mathematical Reasoning [MATH 3000] on Section 4.1. Cardinality; Fundamental Counting Principles).

Theorem 7.1 (continued)

Proof (continued). With $D = \{p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k} \mid 0 \le f_i \le e_i\}$, we see that each f_i may take on $e_1 + 1$ different values. Thus, there are $(e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$ numbers in D and, by the Unique Factorization Theorem (Theorem 2.2, the Fundamental Theorem of Arithmetic), they are all different. (In this claim, we are using the Fundamental Principle of Counting also. See my online notes for Foundations of Probability and Statistics-Calculus Based (MATH 2050) on Section 2.2. Counting Methods [notice Note 2.2.A], my notes for Applied Combinatorics and Problem Solving [MATH 3340] on Section 1.1. The Fundamental Counting Principle, or my notes for Mathematical Reasoning [MATH 3000] on Section 4.1. Cardinality; Fundamental Counting Principles). Since $d(p_i^{e_i}) = e_i + 1$ by Exercise 7.2, then

$$d(n) = (e_1 + 1)(e_2 + 1) \cdots (e_k + 1) = d(p_1^{e_1}) d(p_2^{e_2}) \cdots d(p_k^{e_k}),$$

as claimed. □

Theorem 7.1 (continued)

Proof (continued). With $D = \{p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k} \mid 0 \leq f_i \leq e_i\}$, we see that each f_i may take on $e_1 + 1$ different values. Thus, there are $(e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$ numbers in D and, by the Unique Factorization Theorem (Theorem 2.2, the Fundamental Theorem of Arithmetic), they are all different. (In this claim, we are using the Fundamental Principle of Counting also. See my online notes for Foundations of Probability and Statistics-Calculus Based (MATH 2050) on Section 2.2. Counting Methods [notice Note 2.2.A], my notes for Applied Combinatorics and Problem Solving [MATH 3340] on Section 1.1. The Fundamental Counting Principle, or my notes for Mathematical Reasoning [MATH 3000] on Section 4.1. Cardinality; Fundamental Counting Principles). Since $d(p_i^{e_i}) = e_i + 1$ by Exercise 7.2, then

$$d(n) = (e_1 + 1)(e_2 + 1) \cdots (e_k + 1) = d(p_1^{e_1}) d(p_2^{e_2}) \cdots d(p_k^{e_k}),$$

as claimed. $\square$

Theorem 7.2

Theorem 7.2. If $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime-power decomposition of n, then $\sigma(n) = \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_k^{e_k})$.

Proof. We prove this by induction. The result is trivial for $k = 1$, giving us the base case. For the induction hypothesis, suppose the result holds for $k = r$. Consider $k = r + 1$ and $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} p_{r+1}^{e_{r+1}} = Np^e$, where we let $N = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $p = p_{r+1}$, and $e = e_{r+1}$. Let $1, d_1, d_2, \ldots, d_t$ be the divisors of N. Since $(N, p) = 1$ (the $r + 1$ primes are distinct), all of the divisors of n are of the form of a divisor of N times a divisor of p^e (by Corollaries 1.1 and 1.3).

Theorem 7.2

Theorem 7.2. If $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime-power decomposition of n, then $\sigma(n) = \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_k^{e_k})$.

Proof. We prove this by induction. The result is trivial for $k = 1$, giving us the base case. For the induction hypothesis, suppose the result holds for $k = r$. Consider $k = r + 1$ and $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} p_{r+1}^{e_{r+1}} = Np^e$, where we let $N = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $p = p_{r+1}$, and $e = e_{r+1}$. Let $1, d_1, d_2, \ldots, d_t$ be the divisors of N. Since $(N, p) = 1$ (the $r + 1$ primes are distinct), all of the divisors of n are of the form of a divisor of N times a divisor of p^e (by Corollaries 1.1 and 1.3). So the divisors of n are

$$\begin{array}{ccccc} 1 & d_1 & d_2 & \cdots & d_t \\ p & d_1 p & d_2 p & \cdots & d_t p \\ p^2 & d_1 p^2 & d_2 p^2 & \cdots & d_t p^2 \\ & & & \vdots & \\ p^e & d_1 p^e & d_2 p^e & \cdots & d_t p^e \end{array}$$

Theorem 7.2

Theorem 7.2. If $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime-power decomposition of n, then $\sigma(n) = \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_k^{e_k})$.

Proof. We prove this by induction. The result is trivial for $k = 1$, giving us the base case. For the induction hypothesis, suppose the result holds for $k = r$. Consider $k = r + 1$ and $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} p_{r+1}^{e_{r+1}} = Np^e$, where we let $N = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $p = p_{r+1}$, and $e = e_{r+1}$. Let $1, d_1, d_2, \ldots, d_t$ be the divisors of N. Since $(N, p) = 1$ (the $r + 1$ primes are distinct), all of the divisors of n are of the form of a divisor of N times a divisor of p^e (by Corollaries 1.1 and 1.3). So the divisors of n are

$$\begin{array}{ccccc}
1 & d_1 & d_2 & \cdots & d_t \\
p & d_1 p & d_2 p & \cdots & d_t p \\
p^2 & d_1 p^2 & d_2 p^2 & \cdots & d_t p^2 \\
 & & & \vdots & \\
p^e & d_1 p^e & d_2 p^e & \cdots & d_t p^e
\end{array}$$

Theorem 7.2 (continued)

Theorem 7.2. If $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime-power decomposition of n, then $\sigma(n) = \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_k^{e_k})$.

Proof (continued). Summing the divisors of n we get

$$\sigma(n) = (1 + d_1 + d_2 + \cdots + d_t)(1 + p + p^2 + \cdots + p^e) = \sigma)N)\sigma(p^e).$$

By the induction hypothesis (since $N = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ consists of the product of $k = r$ powers of primes) we have $\sigma(N) = \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_r^{e_r})$. Therefore

$$\sigma(n) = \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_r^{e_r})\sigma(p^e) = \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_r^{e_r})\sigma(p_{r+1}^{e_{r+1}}),$$

giving the induction step. So, by the Principle of Mathematical Induction, the result holds for all $k \in \mathbb{N}$, as claimed. □

Theorem 7.2 (continued)

Theorem 7.2. If $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime-power decomposition of n, then $\sigma(n) = \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_k^{e_k})$.

Proof (continued). Summing the divisors of n we get

$$\sigma(n) = (1 + d_1 + d_2 + \cdots + d_t)(1 + p + p^2 + \cdots + p^e) = \sigma)N)\sigma(p^e).$$

By the induction hypothesis (since $N = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ consists of the product of $k = r$ powers of primes) we have $\sigma(N) = \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_r^{e_r})$. Therefore

$$\sigma(n) = \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_r^{e_r})\sigma(p^e) = \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_r^{e_r})\sigma(p_{r+1}^{e_{r+1}}),$$

giving the induction step. So, by the Principle of Mathematical Induction, the result holds for all $k \in \mathbb{N}$, as claimed. $\square$

Theorem 7.3

Theorem 7.3. d is multiplicative.

Proof. Let m and n be relatively prime (as is required by the definition of "multiplicative"). Then no prime that divides m can divide n and vice versa. So m and n have the prime-power decompositions $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and $n = q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}$ where the p_i's are the q_j's are all distinct. So the prime-power decomposition of mn is $mn = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}$. Then by Theorem 7.1,

$$\begin{aligned} d(mn) &= d(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}) \\ &= d(p_1^{e_1}) d(p_2^{e_2}) \cdots d(p_k^{e_k}) d(q_1^{f_1}) d(q_2^{f_2}) \cdots d(q_r^{f_r}) \\ &= d(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) d(q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}) = d(m)d(n), \end{aligned}$$

as claimed. $\square$

Theorem 7.3

Theorem 7.3. d is multiplicative.

Proof. Let m and n be relatively prime (as is required by the definition of "multiplicative"). Then no prime that divides m can divide n and vice versa. So m and n have the prime-power decompositions $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and $n = q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}$ where the p_i's are the q_j's are all distinct. So the prime-power decomposition of mn is $mn = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}$. Then by Theorem 7.1,

$$\begin{aligned} d(mn) &= d(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}) \\ &= d(p_1^{e_1}) d(p_2^{e_2}) \cdots d(p_k^{e_k}) d(q_1^{f_1}) d(q_2^{f_2}) \cdots d(q_r^{f_r}) \\ &= d(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) d(q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}) = d(m)d(n), \end{aligned}$$

as claimed. □

Theorem 7.4

Theorem 7.4. σ is multiplicative.

Proof. This is virtually identical to the proof of Theorem 7.3. Let m and n be relatively prime. Then no prime that divides m can divide n and vice versa. So m and n have the prime-power decompositions $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and $n = q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}$ where the p_i's are the q_j's are all distinct. So the prime-power decomposition of mn is $mn = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}$. Then by Theorem 7.2,

$$\begin{aligned}
\sigma(mn) &= \sigma(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}) \\
&= \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_k^{e_k})\sigma(q_1^{f_1})\sigma(q_2^{f_2}) \cdots \sigma(q_r^{f_r}) \\
&= \sigma(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k})\sigma(q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}) = \sigma(m)\sigma(n),
\end{aligned}$$

as claimed. $\square$

Theorem 7.4

Theorem 7.4. σ is multiplicative.

Proof. This is virtually identical to the proof of Theorem 7.3. Let m and n be relatively prime. Then no prime that divides m can divide n and vice versa. So m and n have the prime-power decompositions $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and $n = q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}$ where the p_i's are the q_j's are all distinct. So the prime-power decomposition of mn is $mn = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}$. Then by Theorem 7.2,

$$\begin{aligned}
\sigma(mn) &= \sigma(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}) \\
&= \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_k^{e_k})\sigma(q_1^{f_1})\sigma(q_2^{f_2}) \cdots \sigma(q_r^{f_r}) \\
&= \sigma(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k})\sigma(q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}) = \sigma(m)\sigma(n),
\end{aligned}$$

as claimed. □

Theorem 7.5

Theorem 7.5. If f is a multiplicative function and the prime-power decomposition of n is $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then $f(p_1^{e_1}) f(p_2^{e_2}) \cdots f(p_k^{e_k})$.

Proof. We prove this by induction. The result is trivial for $k = 1$, giving us the base case. For the induction hypothesis, suppose the result holds for $k = r$ and that $f(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) = f(p_1^{e_1}) f(p_2^{e_2}) \cdots f(p_r^{e_r})$. Consider the case $k = r + 1$ and the natural number $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} p_{r+1}^{e_{r+1}}$.

Theorem 7.5

Theorem 7.5. If f is a multiplicative function and the prime-power decomposition of n is $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then $f(p_1^{e_1}) f(p_2^{e_2}) \cdots f(p_k^{e_k})$.

Proof. We prove this by induction. The result is trivial for $k = 1$, giving us the base case. For the induction hypothesis, suppose the result holds for $k = r$ and that $f(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) = f(p_1^{e_1}) f(p_2^{e_2}) \cdots f(p_r^{e_r})$. Consider the case $k = r + 1$ and the natural number $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} p_{r+1}^{e_{r+1}}$. We have $(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}, p_{r+1}^{e_{r+1}}) = 1$, so from the definition of a multiplicative function we have

$$f((p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) p_{r+1}^{e_{r+1}}) = f(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) f(p_{r+1}^{e_{r+1}}).$$

By the induction hypothesis we then have

$$f(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} p_{r+1}^{e_{r+1}}) = f(p_1^{e_1}) f(p_2^{e_2}) \cdots f(p_r^{e_r}) f(p_{r+1}^{e_{r+1}}),$$

giving the induction step. So, by the Principle of Mathematical Induction, the result holds for all $k \in \mathbb{N}$, as claimed. □

Theorem 7.5

Theorem 7.5. If f is a multiplicative function and the prime-power decomposition of n is $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then $f(p_1^{e_1}) f(p_2^{e_2}) \cdots f(p_k^{e_k})$.

Proof. We prove this by induction. The result is trivial for $k = 1$, giving us the base case. For the induction hypothesis, suppose the result holds for $k = r$ and that $f(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) = f(p_1^{e_1}) f(p_2^{e_2}) \cdots f(p_r^{e_r})$. Consider the case $k = r + 1$ and the natural number $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} p_{r+1}^{e_{r+1}}$. We have $(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}, p_{r+1}^{e_{r+1}}) = 1$, so from the definition of a multiplicative function we have

$$f((p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) p_{r+1}^{e_{r+1}}) = f(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) f(p_{r+1}^{e_{r+1}}).$$

By the induction hypothesis we then have

$$f(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} p_{r+1}^{e_{r+1}}) = f(p_1^{e_1}) f(p_2^{e_2}) \cdots f(p_r^{e_r}) f(p_{r+1}^{e_{r+1}}),$$

giving the induction step. So, by the Principle of Mathematical Induction, the result holds for all $k \in \mathbb{N}$, as claimed. □