Mathematical Reasoning

Chapter 6. Number Theory

6.9. Perfect Numbers, Mersenne Primes, Arithmetic Functions—Proofs of Theorems

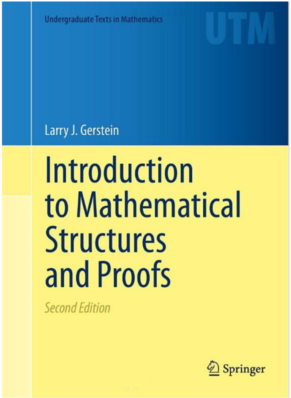

Table of contents

Theorem 6.85

Theorem 6.85. Suppose f is a multiplicative function. Then

(i) $f(1) = 1$, and

(ii) if n has standard factorization $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, then

$$f(n) = \prod_{i=1}^{r} f\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r} f(p_i^{\alpha_i}) = \prod_{i=1}^{r} f(p_i)^{\alpha_i}.$$

Proof. **(i)** By definition of "multiplicative function," there is some $n \in \mathbb{N}$ such that $f(n) \neq 0$. So $f(n) = f(1 \cdot n) = f(1)f(n)$, so dividing by nonzero $f(n)$ gives $f(1) = 1$, as claimed.

Theorem 6.85

Theorem 6.85. Suppose f is a multiplicative function. Then

(i) $f(1) = 1$, and

(ii) if n has standard factorization $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, then

$$f(n) = \prod_{i=1}^{r} f\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r} f(p_i^{\alpha_i}) = \prod_{i=1}^{r} f(p_i)^{\alpha_i}.$$

Proof. **(i)** By definition of "multiplicative function," there is some $n \in \mathbb{N}$ such that $f(n) \neq 0$. So $f(n) = f(1 \cdot n) = f(1)f(n)$, so dividing by nonzero $f(n)$ gives $f(1) = 1$, as claimed.

Theorem 6.85 (continued)

Theorem 6.85. Suppose f is a multiplicative function. Then

(i) $f(1) = 1$, and

(ii) if n has standard factorization $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, then

$$f(n) = \prod_{i=1}^{r} f\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r} f(p_i^{\alpha_i}).$$

Proof (continued). (ii) Since $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, the definition of "multiplicative function" gives

$$f(n) = f\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r} f(p_i^{\alpha_i}),$$

as claimed. □

Theorem 6.89

Theorem 6.89. σ is a multiplicative function.

Proof. Suppose $(m, n) = 1$. If either $m = 1$ or $n = 1$, then $\sigma(mn) = \sigma(m)\sigma(n)$ since $\sigma(1) = 1$. So without loss of generality we can assume that both m and n are greater than 1 and so have standard factorizations $m = \prod_{i=1}^{r} p_i^{\alpha_i}$ and $n = \prod_{j=1}^{s} q_j^{\beta_j}$ with the p'a and q's distinct primes (because $(m, n) = 1$). Now if $d \mid mn$, then $d = \underbrace{p_1^{\nu_1} p_2^{\nu_2} \cdots p_r^{\nu_r}}_{d_1} \underbrace{q_1^{\lambda_1} q_2^{\lambda_2} \cdots q_s^{\lambda_s}}_{d_2}$ with $\nu_i \leq \alpha_i$ and $\lambda_j \leq \beta_j$ for all i and j;

so $d_1 \mid m$, $d_2 \mid n$, and $(d_1, d_2) = 1$. Then

$$\sigma(mn) = \sum_{d \mid mn} d = \sum_{d_1 \mid m, d_2 \mid n} d_1 d_2 = \left(\sum_{d_1 \mid m} d_1 \right) \left(\sum_{d_2 \mid n} d_2 \right) = \sigma(m)\sigma(n),$$

as claimed $\square$

Theorem 6.89

Theorem 6.89. σ is a multiplicative function.

Proof. Suppose $(m,n)=1$. If either $m=1$ or $n=1$, then $\sigma(mn)=\sigma(m)\sigma(n)$ since $\sigma(1)=1$. So without loss of generality we can assume that both m and n are greater than 1 and so have standard factorizations $m=\prod_{i=1}^{r} p_i^{\alpha_i}$ and $n=\prod_{j=1}^{s} q_j^{\beta_j}$ with the p'a and q's distinct primes (because $(m,n)=1$). Now if $d \mid mn$, then

$$d = \underbrace{p_1^{\nu_1} p_2^{\nu_2} \cdots p_r^{\nu_r}}_{d_1} \underbrace{q_1^{\lambda_1} q_2^{\lambda_2} \cdots q_s^{\lambda_s}}_{d_2}$$ with $\nu_i \le \alpha_i$ and $\lambda_j \le \beta_j$ for all i and j;

so $d_1 \mid m$, $d_2 \mid n$, and $(d_1, d_2)=1$. Then

$$\sigma(mn) = \sum_{d \mid mn} d = \sum_{d_1 \mid m, d_2 \mid n} d_1 d_2 = \left(\sum_{d_1 \mid m} d_1\right)\left(\sum_{d_2 \mid n} d_2\right) = \sigma(m)\sigma(n),$$

as claimed □

Corollary 6.90

Corollary 6.90. If $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ then $\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$.

Proof. By Theorem 6.89, σ is multiplicative so we have $\sigma\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r} \sigma(p_i^{\alpha_i})$. Now we consider $\sigma(p^\alpha)$ for p prime and $\alpha \geq 1$. For any x we have $(x-1)(1+x+x^2+\cdots+x^\alpha) = x^{\alpha+1}-1$ (as can be shown inductively or by distribution on the left-hand side). So with $x = p$ we have $\sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha = \frac{p^{\alpha+1}-1}{p-1}$. Then

$$\sigma(n) = \prod_{i=1}^{r} \sigma(p_i^{\alpha_i}) = \prod_{i=1}^{r} \frac{p^{\alpha+1}-1}{p-1},$$

as claimed. □

Corollary 6.90

Corollary 6.90. If $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ then $\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$.

Proof. By Theorem 6.89, σ is multiplicative so we have $\sigma\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r} \sigma(p_i^{\alpha_i})$. Now we consider $\sigma(p^\alpha)$ for p prime and $\alpha \geq 1$. For any x we have $(x-1)(1+x+x^2+\cdots+x^\alpha) = x^{\alpha+1} - 1$ (as can be shown inductively or by distribution on the left-hand side). So with $x = p$ we have $\sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}$. Then

$$\sigma(n) = \prod_{i=1}^{r} \sigma(p_i^{\alpha_i}) = \prod_{i=1}^{r} \frac{p^{\alpha+1} - 1}{p - 1},$$

as claimed. □

Exercise 6.93

Exercise 6.93. Prove that if n is positive and composite, then $2^n - 1$ is not prime. That is, for $2^n - 1$ to be prime, it is necessary that n is prime.

Proof. Suppose n is a positive composite number, say $n = k\ell$ where k and ℓ are positive and greater than 1. As commented in the proof of Corollary 6.90, any all x we have $(x-1)(1+x+x^2+\cdots+x^\alpha) = x^{\alpha+1} - 1$. With $x = 2^k$ and $\alpha = n - 1 = k\ell - 1$ we have

$$(2^k - 1)(1 + 2^k + 2^{2k} + \cdots + 2^{k\ell-1}) = 2^{(k\ell-1)+1} - 1 = 2^{k\ell} - 1 = 2^n - 1.$$

So $2^k - 1$ (which is at least 3) is a divisor of $2^n - 1$ and $2^n - 1$ is not prime, as claimed. □

Exercise 6.93

Exercise 6.93. Prove that if n is positive and composite, then $2^n - 1$ is not prime. That is, for $2^n - 1$ to be prime, it is necessary that n is prime.

Proof. Suppose n is a positive composite number, say $n = k\ell$ where k and ℓ are positive and greater than 1. As commented in the proof of Corollary 6.90, any all x we have $(x-1)(1+x+x^2+\cdots+x^\alpha) = x^{\alpha+1}-1$. With $x = 2^k$ and $\alpha = n-1 = k\ell - 1$ we have

$$(2^k-1)(1+2^k+2^{2k}+\cdots+2^{k\ell-1}) = 2^{(k\ell-1)+1}-1 = 2^{k\ell}-1 = 2^n-1.$$

So $2^k - 1$ (which is at least 3) is a divisor of $2^n - 1$ and $2^n - 1$ is not prime, as claimed. □

Theorem 6.94. Euclid-Euler Theorem

Theorem 6.94. Euclid-Euler Theorem.
A positive even integer n is perfect if and only if there is a factorization $n = 2^{p-1}(2^p - 1)$ with p prime and $2^p - 1$ a Mersenne prime.

Proof. First, suppose $n = 2^{p-1}(2^p - 1)$, with $2^p - 1$ a Mersenne prime. Then n is even and since σ is multiplicative by Theorem 6.89 ($2^p - 1$ and $2^p - 1$ are certainly relatively prime), then $\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1)$. But $\sigma(2^{p-1}) = 1 + 2 + 2^2 + \cdots + 2^{p-1} = 2^p - 1$, and $\sigma(2^p - 1) = 2^p$ because $2^p - 1$ is prime by hypothesis (see Example 6.88).

Theorem 6.94. Euclid-Euler Theorem

Theorem 6.94. Euclid-Euler Theorem.
A positive even integer n is perfect if and only if there is a factorization $n = 2^{p-1}(2^p - 1)$ with p prime and $2^p - 1$ a Mersenne prime.

Proof. First, suppose $n = 2^{p-1}(2^p - 1)$, with $2^p - 1$ a Mersenne prime. Then n is even and since σ is multiplicative by Theorem 6.89 ($2^p - 1$ and $2^p - 1$ are certainly relatively prime), then $\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1)$. But $\sigma(2^{p-1}) = 1 + 2 + 2^2 + \cdots + 2^{p-1} = 2^p - 1$, and $\sigma(2^p - 1) = 2^p$ because $2^p - 1$ is prime by hypothesis (see Example 6.88). So $\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1) = (2^p - 1) \cdot 2^p = 2 \cdot 2^{p-1}(2^p - 1) = 2n$ and hence n is perfect, as claimed. Notice that this is a proof of Euclid's result in Book IX, Proposition 36 of the *Elements*.

Theorem 6.94. Euclid-Euler Theorem

Theorem 6.94. Euclid-Euler Theorem.
A positive even integer n is perfect if and only if there is a factorization $n = 2^{p-1}(2^p - 1)$ with p prime and $2^p - 1$ a Mersenne prime.

Proof. First, suppose $n = 2^{p-1}(2^p - 1)$, with $2^p - 1$ a Mersenne prime. Then n is even and since σ is multiplicative by Theorem 6.89 ($2^p - 1$ and $2^p - 1$ are certainly relatively prime), then $\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1)$. But $\sigma(2^{p-1}) = 1 + 2 + 2^2 + \cdots + 2^{p-1} = 2^p - 1$, and $\sigma(2^p - 1) = 2^p$ because $2^p - 1$ is prime by hypothesis (see Example 6.88). So $\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1) = (2^p - 1) \cdot 2^p = 2 \cdot 2^{p-1}(2^p - 1) = 2n$ and hence n is perfect, as claimed. Notice that this is a proof of Euclid's result in Book IX, Proposition 36 of the *Elements*.

Theorem 6.94. Euclid-Euler Theorem (continued 1)

Proof (continued). Conversely, suppose n is an even perfect number; say $n = 2^k m$ where $k \geq 1$ and m is odd. Since n is perfect by hypothesis, we have $\sigma(n) = 2n = 2^{k+1}m$. Now 2^k and m are relatively prime, σ is multiplicative by Theorem 6.89, and by Corollary 6.90 (with $r = 1$, $p_1 = 2$, and $\alpha_1 = k$) we have $\sigma(2^k) = 2^{k+1} - 1$, so we also have

$$\sigma(n) = \sigma(2^k)\sigma(m) = (2^{k+1} - 1)\sigma(m).$$

Therefore $2^{k+1}m = (2^{k+1} - 1)\sigma(m)$. Since 2^{k+1} and $2^{k+1} - 1$ are relatively prime, then this implies that $2^{k+1} \mid \sigma(m)$, say $\sigma(m) = 2^{k+1}c$. Then $2^{k+1}m = (2^{k+1} - 1)2^{k+1}c$, which implies that $m = (2^{k+1} - 1)c$ and c is a divisor of m. Also,

$$m = (2^{k+1} - 1)c = 2^{k+1}c - c = \sigma(m) - c.$$

Therefore $\sigma(m) = m + c$.

Theorem 6.94. Euclid-Euler Theorem (continued 1)

Proof (continued). Conversely, suppose n is an even perfect number; say $n = 2^k m$ where $k \geq 1$ and m is odd. Since n is perfect by hypothesis, we have $\sigma(n) = 2n = 2^{k+1}m$. Now 2^k and m are relatively prime, σ is multiplicative by Theorem 6.89, and by Corollary 6.90 (with $r = 1$, $p_1 = 2$, and $\alpha_1 = k$) we have $\sigma(2^k) = 2^{k+1} - 1$, so we also have

$$\sigma(n) = \sigma(2^k)\sigma(m) = (2^{k+1} - 1)\sigma(m).$$

Therefore $2^{k+1}m = (2^{k+1} - 1)\sigma(m)$. Since 2^{k+1} and $2^{k+1} - 1$ are relatively prime, then this implies that $2^{k+1} \mid \sigma(m)$, say $\sigma(m) = 2^{k+1}c$. Then $2^{k+1}m = (2^{k+1} - 1)2^{k+1}c$, which implies that $m = (2^{k+1} - 1)c$ and c is a divisor of m. Also,

$$m = (2^{k+1} - 1)c = 2^{k+1}c - c = \sigma(m) - c.$$

Therefore $\sigma(m) = m + c$.

Theorem 6.94. Euclid-Euler Theorem (continued 2)

Theorem 6.94. Euclid-Euler Theorem.
A positive even integer n is perfect if and only if there is a factorization $n = 2^{p-1}(2^p - 1)$ with p prime and $2^p - 1$ a Mersenne prime.

Proof (continued). Denote the divisors of m as $d_1 = 1, d_2, d_3, \ldots, d_\ell, d_{\ell+1} = m$; since c is a divisor of m and $c < m$, then c is one of $1, d_2, d_3, \ldots, d_\ell$. Since $\sigma(m) = m + c$ from above, we now have

$$m + c = \sigma(m) = 1 + d_2 + d_3 + \cdots + d_\ell + m,$$

so that $c = 1 + d_2 + d_3 + \cdots + d_\ell$ where c is one of the terms on the right-hand side of this equation. This can only be the case if $c = 1$ (for if $c \neq 1$, then $c = 1 + c +$ (possibly other positive terms), a contradiction). So we have $m = (2^{k+1} - 1)c = 2^{k+1} - 1$ and $\sigma(m) = m + c = m + 1$. Therefore, the only divisors of m are 1 and m itself, so that m is a prime of the form $2^{k+1} - 1$. By Exercise 6.93, we see that $k + 1$ must be prime, say $p = k + 1$. Hence m is a Mersenne prime. Also, we have $n = 2^k m = 2^{p-1}(2^p - 1)$, as claimed. □

Theorem 6.94. Euclid-Euler Theorem (continued 2)

Theorem 6.94. Euclid-Euler Theorem.
A positive even integer n is perfect if and only if there is a factorization $n = 2^{p-1}(2^p - 1)$ with p prime and $2^p - 1$ a Mersenne prime.

Proof (continued). Denote the divisors of m as $d_1 = 1, d_2, d_3, \ldots, d_\ell, d_{\ell+1} = m$; since c is a divisor of m and $c < m$, then c is one of $1, d_2, d_3, \ldots, d_\ell$. Since $\sigma(m) = m + c$ from above, we now have

$$m + c = \sigma(m) = 1 + d_2 + d_3 + \cdots + d_\ell + m,$$

so that $c = 1 + d_2 + d_3 + \cdots + d_\ell$ where c is one of the terms on the right-hand side of this equation. This can only be the case if $c = 1$ (for if $c \neq 1$, then $c = 1 + c +$ (possibly other positive terms), a contradiction). So we have $m = (2^{k+1} - 1)c = 2^{k+1} - 1$ and $\sigma(m) = m + c = m + 1$. Therefore, the only divisors of m are 1 and m itself, so that m is a prime of the form $2^{k+1} - 1$. By Exercise 6.93, we see that $k + 1$ must be prime, say $p = k + 1$. Hence m is a Mersenne prime. Also, we have $n = 2^k m = 2^{p-1}(2^p - 1)$, as claimed. □

Lemma 6.96

Lemma 6.96. Suppose $n \in \mathbb{N}$. Then $\displaystyle\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}$

Proof. If $n = 1$, then $\mu(n) = \mu(1) = 1$ by the definition of $\mu(1)$ (the first part). If $n = p$ a prime, then $\sum_{d \mid p} \mu(d) = \mu(1) + \mu(p) = 1 + (-1)^1 = 0$, as claimed. Now suppose n has standard factorization $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, with $r \geq 1$ and $\alpha_i \geq 1$ for all i. If a divisor d of n divides the product $p_1 p_2 \cdots p_r$, then by the definition of $\mu(d)$ (the second part) we have $\mu(d) = \pm 1$ (the depending on how many primes are in the standard factorization of d, even or odd respectively).

Lemma 6.96

Lemma 6.96. Suppose $n \in \mathbb{N}$. Then $\displaystyle\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}$

Proof. If $n = 1$, then $\mu(n) = \mu(1) = 1$ by the definition of $\mu(1)$ (the first part). If $n = p$ a prime, then $\sum_{d \mid p} \mu(d) = \mu(1) + \mu(p) = 1 + (-1)^1 = 0$, as claimed. Now suppose n has standard factorization $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, with $r \geq 1$ and $\alpha_i \geq 1$ for all i. If a divisor d of n divides the product $p_1 p_2 \cdots p_r$, then by the definition of $\mu(d)$ (the second part) we have $\mu(d) = \pm 1$ (the depending on how many primes are in the standard factorization of d, even or odd respectively). For all *other* divisors d of n (if such divisors exist) we have $\mu(d) = 0$ by the definition of $\mu(d)$ (the third part; since such divisors must be divisible by some square of at least one prime). Now the divisors of $p_1 p_2 \cdots p_r$ are all of the form $p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_r^{\varepsilon_r}$ with $\varepsilon_i \in \{0, 1\}$ for all i.

Lemma 6.96

Lemma 6.96. Suppose $n \in \mathbb{N}$. Then $\displaystyle\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}$

Proof. If $n = 1$, then $\mu(n) = \mu(1) = 1$ by the definition of $\mu(1)$ (the first part). If $n = p$ a prime, then $\sum_{d \mid p} \mu(d) = \mu(1) + \mu(p) = 1 + (-1)^1 = 0$, as claimed. Now suppose n has standard factorization $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, with $r \geq 1$ and $\alpha_i \geq 1$ for all i. If a divisor d of n divides the product $p_1 p_2 \cdots p_r$, then by the definition of $\mu(d)$ (the second part) we have $\mu(d) = \pm 1$ (the depending on how many primes are in the standard factorization of d, even or odd respectively). For all *other* divisors d of n (if such divisors exist) we have $\mu(d) = 0$ by the definition of $\mu(d)$ (the third part; since such divisors must be divisible by some square of at least one prime). Now the divisors of $p_1 p_2 \cdots p_r$ are all of the form $p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_r^{\varepsilon_r}$ with $\varepsilon_i \in \{0, 1\}$ for all i.

Lemma 6.96 (continued)

Proof (continued). There are $\binom{r}{k}$ of these divisors in which exactly k of the exponents ε_i are equal to 1 (the number of ways we can choose the subscripts for the value-one exponents, the value-zero exponents then being determined by default). Equivalently, there are $\binom{r}{k}$ divisors of $p_1 p_2 \cdots p_r$ having exactly k prime factors. For each such divisor d we have

$$\mu(d) = (-1)^k = \begin{cases} 1 & \text{if } k \text{ is even} \\ -1 & \text{if } k \text{ is odd,} \end{cases}$$

by the definition of $\mu(d)$ (the second part). We therefore have, by the Binomial Theorem (see Theorem 5.73),

$$\sum_{d \mid n} \mu(d) = \sum_{d \mid p_1 p_2 \cdots p_r} \mu(d) = \sum_{k=0}^{r} \binom{r}{k} (-1)^k = \sum_{k=0}^{r} \binom{r}{k} (1)^{r-k} (-1)^k = 0,$$

as claimed. □

Lemma 6.96 (continued)

Proof (continued). There are $\binom{r}{k}$ of these divisors in which exactly k of the exponents ε_i are equal to 1 (the number of ways we can choose the subscripts for the value-one exponents, the value-zero exponents then being determined by default). Equivalently, there are $\binom{r}{k}$ divisors of $p_1 p_2 \cdots p_r$ having exactly k prime factors. For each such divisor d we have

$$\mu(d) = (-1)^k = \begin{cases} 1 & \text{if } k \text{ is even} \\ -1 & \text{if } k \text{ is odd,} \end{cases}$$

by the definition of $\mu(d)$ (the second part). We therefore have, by the Binomial Theorem (see Theorem 5.73),

$$\sum_{d \mid n} \mu(d) = \sum_{d \mid p_1 p_2 \cdots p_r} \mu(d) = \sum_{k=0}^{r} \binom{r}{k} (-1)^k = \sum_{k=0}^{r} \binom{r}{k} (1)^{r-k} (-1)^k = 0,$$

as claimed. □

Theorem 6.97. Möbius-Inversion Formula

Theorem 6.97. Möbius-Inversion Formula.
Let f be an arithmetic function, and suppose $g(n) = \sum_{d \mid n} f(d)$ for all $n \in \mathbb{N}$. Then

$$f(n) = \sum_{d \mid n} \mu(d) g(n/d).$$

Proof. First, if $d \mid n$ then $n = cd$ for $c = n/d$ is a divisor of n (and vice versa). We have

$$\begin{aligned} \sum_{d \mid n} \mu(d) g(n/d) &= \sum_{d \mid n} \left(\mu(d) \sum_{c \mid n/d} f(c) \right) \text{ by the definition of } g \\ &= \sum_{d \mid n,\ c \mid n/d} \mu(d) f(c) \text{ distributing} \\ &= \sum_{cd = n} \mu(d) f(c) = \sum_{c \mid n} \left(f(c) \sum_{d \mid n/c} \mu(d) \right) \text{ factoring.} \end{aligned}$$

Theorem 6.97. Möbius-Inversion Formula

Theorem 6.97. Möbius-Inversion Formula.
Let f be an arithmetic function, and suppose $g(n) = \sum_{d \mid n} f(d)$ for all $n \in \mathbb{N}$. Then

$$f(n) = \sum_{d \mid n} \mu(d) g(n/d).$$

Proof. First, if $d \mid n$ then $n = cd$ for $c = n/d$ is a divisor of n (and vice versa). We have

$$\begin{aligned} \sum_{d \mid n} \mu(d) g(n/d) &= \sum_{d \mid n} \left(\mu(d) \sum_{c \mid n/d} f(c) \right) \text{ by the definition of } g \\ &= \sum_{d \mid n,\ c \mid n/d} \mu(d) f(c) \text{ distributing} \\ &= \sum_{cd=n} \mu(d) f(c) = \sum_{c \mid n} \left(f(c) \sum_{d \mid n/c} \mu(d) \right) \text{ factoring.} \end{aligned}$$

Theorem 6.97. Möbius-Inversion Formula (continued)

Theorem 6.97. Möbius-Inversion Formula.
Let f be an arithmetic function, and suppose $g(n) = \sum_{d \mid n} f(d)$ for all $n \in \mathbb{N}$. Then

$$f(n) = \sum_{d \mid n} \mu(d) g(n/d).$$

Proof (continued). $\ldots \sum_{d \mid n} \mu(d) g(n/d) = \sum_{c \mid n} \left(f(c) \sum_{d \mid n/c} \mu(d) \right)$. By Lemma 6.96 we have $\sum_{d \mid n/c} \mu(d) = 0$ unless $d = 1$ (that is, $c = n$). So in the right-most term in the equation above, only the term with $c = n$ is nonzero. When $c = n$, the right-most term is $f(n)\mu(1) = f(n)$. That is,

$$\sum_{d \mid n} \mu(d) g(n/d) = \sum_{c \mid n} \left(f(c) \sum_{d \mid n/c} \mu(d) \right) = f(n),$$

as claimed. □

Lemma 6.98

Lemma 6.98. If $n \in \mathbb{N}$, then $\displaystyle\sum_{d \mid n} \varphi(d) = n$.

Proof. Let $n \in \mathbb{N}$ be given. For the set of integers $S = \{1, 2, \ldots, n\}$, define the set C_d (where $1 \leq d \leq n$) to consist of those numbers in S that have greatest common divisor with n or d. That is, for given n we have $m \in C_d$ if and only if $(m, n) = d$. But $(m, n) = d$ if and only if $(m/d, n/d) = 1$. So $m \in C_d$ if and only if m/d is relatively prime to n/d.

Lemma 6.98

Lemma 6.98. If $n \in \mathbb{N}$, then $\displaystyle\sum_{d \mid n} \varphi(d) = n$.

Proof. Let $n \in \mathbb{N}$ be given. For the set of integers $S = \{1, 2, \ldots, n\}$, define the set C_d (where $1 \le d \le n$) to consist of those numbers in S that have greatest common divisor with n or d. That is, for given n we have $m \in C_d$ if and only if $(m, n) = d$. But $(m, n) = d$ if and only if $(m/d, n/d) = 1$. So $m \in C_d$ if and only if m/d is relatively prime to n/d. The number of positive integers less than or equal to n/d and relatively prime to n/d is, by definition, $\varphi(n/d)$. So the number of elements in C_d is $\varphi(n/d)$. Since each element of $S = \{1, 2, \ldots, n\}$ is in exactly one C_d, then $n = \sum_{d \mid n} \varphi(n/d)$. Now if $d \mid n$, then $n = dc$ for some c where $c \mid n$ (and $c = n/d$). So summing $\varphi(n/d)$ over all $d \mid n$, is equivalent to summing $\varphi(c)$ over all $c \mid n$. That is, $\sum_{d \mid n} \varphi(n/d) = \sum_{c \mid n} \varphi(c)$. So $n = \sum_{d \mid n} \varphi(n/d) = \sum_{d \mid n} \varphi(d)$, as claimed. □

Lemma 6.98

Lemma 6.98. If $n \in \mathbb{N}$, then $\displaystyle\sum_{d \mid n} \varphi(d) = n$.

Proof. Let $n \in \mathbb{N}$ be given. For the set of integers $S = \{1, 2, \ldots, n\}$, define the set C_d (where $1 \leq d \leq n$) to consist of those numbers in S that have greatest common divisor with n or d. That is, for given n we have $m \in C_d$ if and only if $(m, n) = d$. But $(m, n) = d$ if and only if $(m/d, n/d) = 1$. So $m \in C_d$ if and only if m/d is relatively prime to n/d. The number of positive integers less than or equal to n/d and relatively prime to n/d is, by definition, $\varphi(n/d)$. So the number of elements in C_d is $\varphi(n/d)$. Since each element of $S = \{1, 2, \ldots, n\}$ is in exactly one C_d, then $n = \sum_{d \mid n} \varphi(n/d)$. Now if $d \mid n$, then $n = dc$ for some c where $c \mid n$ (and $c = n/d$). So summing $\varphi(n/d)$ over all $d \mid n$, is equivalent to summing $\varphi(c)$ over all $c \mid n$. That is, $\sum_{d \mid n} \varphi(n/d) = \sum_{c \mid n} \varphi(c)$. So $n = \sum_{d \mid n} \varphi(n/d) = \sum_{d \mid n} \varphi(d)$, as claimed. □

Theorem 6.99

Theorem 6.99.
(i) If n has standard factorization $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, then

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

(ii) φ is multiplicative.

Proof. Define the identity function $g(n) = n$ for all $n \in \mathbb{N}$. Then by Lemma 6.98 we have $g(n) = n = \sum_{d \mid n} \varphi(d)$, so the Möbius inversion formula (with f as φ) yields

$$\varphi(n) = \sum_{d \mid n} \mu(d) g(n/d) = \sum_{d \mid n} \mu(d)(n/d) = \sum_{d \mid p_1 p_2 \cdots p_r} n\mu(d)/d,$$

since $\mu(d) = 0$ for any divisor d that is not a divisor of $p_1 p_2 \cdots p_r$, since such d would not be square-free (μ is a Möbius function).

Theorem 6.99

Theorem 6.99.
(i) If n has standard factorization $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, then

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

(ii) φ is multiplicative.

Proof. Define the identity function $g(n) = n$ for all $n \in \mathbb{N}$. Then by Lemma 6.98 we have $g(n) = n = \sum_{d \mid n} \varphi(d)$, so the Möbius inversion formula (with f as φ) yields

$$\varphi(n) = \sum_{d \mid n} \mu(d) g(n/d) = \sum_{d \mid n} \mu(d)(n/d) = \sum_{d \mid p_1 p_2 \cdots p_r} n\mu(d)/d,$$

since $\mu(d) = 0$ for any divisor d that is not a divisor of $p_1 p_2 \cdots p_r$, since such d would not be square-free (μ is a Möbius function).

Theorem 6.99 (continued 1)

Proof (continued). Now $n\mu(1)/1 = n$, while if $d \mid p_1 p_2 \cdots p_r$ and $d \neq 1$ then d is a product of the form $p_{i_1} p_{i_2} \cdots p_{i_t}$ with $1 \leq t \leq r$ and (say) $p_{i_1} < p_{i_2} < \cdots < p_{i_t}$ so that (by the definition of Möbius function μ) $\mu(d) = (-1)^t$. Therefore

$$\sum_{d \mid p_1 p_2 \cdots p_r} n\mu(d)/d = n - \sum_i \frac{n}{p_1} + \sum_{i_1 < i_2} \frac{n}{p_{i_1} p_{i_2}}$$

$$+ \sum_{i_1 < i_2 < i_3} \frac{n}{p_{i_1} p_{i_2} p_{i_3}} + \cdots + (-1)^r \sum_{i_1 < i_2 < \cdots < i_r} \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_r}}$$

$$= n \left(1 - \sum_i \frac{1}{p_1} + \sum_{i_1 < i_2} \frac{1}{p_{i_1} p_{i_2}} + \sum_{i_1 < i_2 < i_3} \frac{1}{p_{i_1} p_{i_2} p_{i_3}} + \cdots \right.$$

$$\left. + (-1)^r \sum_{i_1 < i_2 < \cdots < i_r} \frac{1}{p_{i_1} p_{i_2} \cdots p_{i_r}} \right) = n \prod_{i=1}^{r} \left(1 = \frac{1}{p_i} \right) \ldots$$

Theorem 6.99 (continued 2)

Theorem 6.99.
(i) If n has standard factorization $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, then

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

(ii) φ is multiplicative.

Proof (continued). . . . where the last equality holds by the Principle of Mathematical Induction. Therefore,

$$\varphi(n) = \sum_{d \mid n} \mu(d) g(n/d) = \sum_{d \mid n} \mu(d)(n/d) = n \prod_{i=1}^{r} \left(1 = \frac{1}{p_i}\right),$$

as claimed.

(ii) This was proved in the "moreover" claim in proof of Theorem 6.59. □

Theorem 6.99 (continued 2)

Theorem 6.99.
(i) If n has standard factorization $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, then

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

(ii) φ is multiplicative.

Proof (continued). ...where the last equality holds by the Principle of Mathematical Induction. Therefore,

$$\varphi(n) = \sum_{d \mid n} \mu(d) g(n/d) = \sum_{d \mid n} \mu(d)(n/d) = n \prod_{i=1}^{r} \left(1 = \frac{1}{p_i}\right),$$

as claimed.

(ii) This was proved in the "moreover" claim in proof of Theorem 6.59. □

Theorem 6.101

Theorem 6.101. If f and g are multiplicative functions, then $f * g$ is multiplicative.

Proof. Suppose $(a, b) = 1$. Then the divisors of ab are the numbers of the form $d = d_1 d_2$ with $d_1 \mid a$ and $d_2 \mid b$. We have by the definition of $f * g$,

$$(f * g)(ab) = \sum_{d \mid ab} f(d) g(ab/d) = \sum_{d_1 \mid a,\ d_2 \mid b} f(d_1 d_2) g(ab/(d_1 d_2))$$

$$= \sum_{d_1 \mid a,\ d_2 \mid b} f(d_1) f(d_2) g(a/d_1) g(b/d_2),$$

because f and g are multiplicative.

Theorem 6.101

Theorem 6.101. If f and g are multiplicative functions, then $f * g$ is multiplicative.

Proof. Suppose $(a, b) = 1$. Then the divisors of ab are the numbers of the form $d = d_1 d_2$ with $d_1 \mid a$ and $d_2 \mid b$. We have by the definition of $f * g$,

$$(f * g)(ab) = \sum_{d \mid ab} f(d)g(ab/d) = \sum_{d_1 \mid a,\ d_2 \mid b} f(d_1 d_2)g(ab/(d_1 d_2))$$

$$= \sum_{d_1 \mid a,\ d_2 \mid b} f(d_1)f(d_2)g(a/d_1)g(b/d_2),$$

because f and g are multiplicative.

Theorem 6.101 (continued)

Theorem 6.101. If f and g are multiplicative functions, then $f * g$ is multiplicative.

Proof (continued). So

$$\begin{aligned}(f*g)(ab) &= \sum_{d_1 \mid a,\ d_2 \mid b} f(d_1)f(d_2)g(a/d_1)g(b/d_2) \\ &= \left(\sum_{d_1 \mid a} f(d_1)g(a/d_1)\right)\cdot\left(\sum_{d_2 \mid b} f(d_2)g(b/d_1)\right) \text{ factoring} \\ &= (f*g)(a)\cdot(f*g)(b),\end{aligned}$$

so that $f * g$ is multiplicative, as claimed. □