5 Multiplicative Functions

For further reading on the material in this subsection, consult **Rosen 7.1, Stein 2.2**.

Definition 5.1. An *arithmetic function* is a function defined for all natural numbers.

A function is *multiplicative* if it has the property that $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$. It is *completely multiplicative* if $f(mn) = f(m)f(n)$ for all natural numbers m, n.

Example 5.2. The functions $f(n) = 1$ and $g(n) = n$ are completely multiplicative.

We will see that $\phi(n)$ is multiplicative but not completely multiplicative. (Example: $\phi(4) = 2 \neq 1 \cdot 1 = \phi(2) \cdot \phi(2)$).

Completely multiplicative functions are easy to understand, but we can get a good grasp even of regularly multiplicative functions.

Proposition 5.3. *If f is multiplicative and $n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s} = \prod_{i=1}^s p_i^{a_i}$ is the prime factorization of n, then*

$$f(n) = f(p_1^{a_1}) f(p_2^{a_2}) \dots f(p_s^{a_s}) = \prod_{i=1}^{s} f(p_i^{a_i}).$$

Proof. We prove by induction on s, the number of distinct prime factors of n. If $s = 1$ then $n = p_1^{a_1}$ and then $f(n) = f(p_1^{a_1})$ is trivially true.

Suppose the proposition is true for all integers with k distinct prime factors, and suppose n has $k+1$ distinct prime factors, say $n = \prod_{i=1}^{k+1} p_i^{a_i}$. We observe that $\left(\prod_{i=1}^k p_i^{a_i}, p_{k+1}^{a_{k+1}}\right) = 1$, and thus by definition of a multiplicative function we know that

$$f\left(\prod_{i=1}^{k+1} p_i^{a_i}\right) = f\left(\prod_{i=1}^{k} p_i^{a_i}\right) f(p_{k+1}^{a_{k+1}}).$$

And by inductive hypothesis we know that

$$f\left(\prod_{i=1}^{k} p_i^{a_i}\right) = \prod_{i=1}^{k} f(p_i^{a_i})$$

and thus we have

$$f\left(\prod_{i=1}^{k+1} p_i^{a_i}\right) = \prod_{i=1}^{k} f(p_i^{a_i}) f(p_{k+1}^{a_{k+1}}) = \prod_{i=1}^{k+1} f(p_i^{a_i}).$$

□

Thus for any multiplicative function, if we can compute its value for prime powers, we can easily compute its value for any number.

5.1 The Euler ϕ-function

For further reading on the material in this subsection, consult **Rosen 7.1, Stein 2.2**.

We want to understand the Euler ϕ-function much better. We will prove that it is a multiplicative function (though, as we observed earlier, it is not completely multiplicative). After that we'll figure out how to compute ϕ of prime powers, which will allow us to easily compute $\phi(n)$ for any positive integer n.

Proposition 5.4. *Let m, n be relative prime natural numbers. Then $\phi(mn) = \phi(m)\phi(n)$. In other words, the function $\phi(n)$ is multiplicative.*

Proof. Write the numbers $\leq mn$ as follows:

$$\begin{array}{ccccc}
1 & m+1 & 2m+1 & \dots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \dots & (n-1)m+2 \\
3 & m+3 & 2m+3 & \dots & (n-1)m+3 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
r & m+r & 2m+r & \dots & (n-1)m+r \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
m & 2m & 3m & \dots & nm
\end{array}$$

Note that $(km + r, m) = (r, m)$, thus the first element of a given row is relatively prime to m if and only if *every* element of that row is. Since $(r, m) > 1$ implies that $(r, mn) > 1$, we only need to consider elements in rows r where $(r, m) = 1$. There are, of course, $\phi(m)$ such rows.

Now suppose $(r, m) = 1$ and consider the elements of this row, which are $km + r$ for $0 \leq k \leq n - 1$. We claim this is a complete system of residues modulo n. It's enough to prove that no two elements are congruent to each other, by HW 4 problem 2. But if $im + r \equiv jm + r \mod n$ then $n | m(i - j)$, and since $(n, m) = 1$, by Euclid's lemma this implies $n | i - j$. But $i, j < n$, so $i = j$.

Since this is a complete system of residues, exactly $\phi(n)$ of these integers are relatively prime to n. Since these integers are also relatively prime to m, they are relatively prime to mn.

Thus there are $\phi(m)$ rows that contain any elements relatively prime to mn; each such row contains $\phi(n)$ such elements. Thus there are in total $\phi(m)\phi(n)$ natural numbers relatively prime to mn and $\leq mn$; but this is the definition of $\phi(mn)$. □

Now that we know $\phi(n)$ is a multiplicative function, we know we can compute it purely by computing its value at prime powers. So we turn our attention to computing $\phi(p^k)$. First, recall from homework that $\phi(n) = n - 1$ if and only if n is prime.

Lemma 5.5. *Let p be a prime number, and let k be a positive integer. Then $\phi(p^k) = p^k - p^{k-1}$.*

Proof. An integer is relatively prime to p^k if and only if it is divisible by p. Thus the integers $n \leq p^k$ which are *not* relatively prime to p^k are the integers ℓp for $1 \leq \ell \leq p^{k-1}$. There are of course p^{k-1} such integers, and there are p^k total integers $n \leq p^k$; thus there are $p^k - p^{k-1}$ integers $n \leq p^k$ such that $(n, p^k) = 1$. □

Example 5.6. $\phi(2^{10}) = 2^{10} - 2^9 = 1024 - 512 = 512$.

$\phi(7^3) = 7^3 - 7^2 = 343 - 49 = 298$.

Theorem 5.7. *Let $n = \prod_{i=1}^k p_i^{a_i}$ be the prime factorization of a natural number. Then*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right) = n\prod_{i=1}^k\left(1 - \frac{1}{p_i}\right).$$

Proof. By proposition 5.3, we know that

$$\phi(n) = \prod_{i=1}^k \phi(p_i^{a_i}).$$

But by lemma 5.5 we know that

$$\phi(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i - 1} = p_i^{a_i}\left(1 - \frac{1}{p_i}\right).$$

Thus

$$\begin{aligned}\phi(n) = \prod_{i=1}^k \phi(p_i^{a_i}) &= \prod_{i=1}^k p_i^{a_i}\left(1 - \frac{1}{p_i}\right) \\ &= \left(\prod_{i=1}^k p_i^{a_i}\right)\left(\prod_{i=1}^k\left(1 - \frac{1}{p_i}\right)\right) \\ &= n\prod_{i=1}^k\left(1 - \frac{1}{p_i}\right).\end{aligned}$$

□

Example 5.8.

$$\phi(100) = \phi(2^2 \cdot 5^2) = 100(1 - 1/2)(1 - 1/5) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40.$$

$$\phi(360) = \phi(2^3 \cdot 3^2 \cdot 5) = 360(1 - 1/2)(1 - 1/3)(1 - 1/5) = 360\frac{8}{30} = 96.$$

Corollary 5.9. *If $n > 2$ then $\phi(n)$ is even.*

Proof. Let $n = \prod_{i=1}^k p_i^{a_i}$. Then $\phi(n) = \prod_{i=1}^k \phi(p_i^{a_i})$.

Suppose n has an odd prime factor p_k. Then since $p_k^{a_k}$ and $p_k^{a_k-1}$ are both odd, $2 | p_k^{a_k} - p_k^{a_k-1} = \phi(p_k) | \phi(n)$.

Now suppose n has no odd prime factors. Then $n = 2^r$ and $r > 1$. Then $\phi(n) = 2^r - 2^{r-1} = 2^{r-1}$ is even. □

This opens up an additional question: given an integer m, for what n is $\phi(n) = m$?

Example 5.10. What are the solutions to the equation $\phi(n) = 8$?

Suppose $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$. Then we have the equation

$$\phi(n) = \prod_{j=1}^k p_j^{a_j - 1}(p_j - 1)$$

which is just a restatement of theorem 5.7. Then the only primes that can divide n are 2, 3, and 5, since we know that $p_i - 1 | n$. Further, if $a_i > 1$ then $p_i | n$, so we know that 3 and 5 can each divide n at most once. Thus we have $n = 2^{a_2} 3^{a_3} 5^{a_5}$, and a_3, a_5 are either 0 or 1.

Suppose $a_3 = a_5 = 0$ so that $n = 2^{a_2}$. Then $\phi(n) = \phi(2^{a_2}) = 2^{a_2 - 1}(2-1)$, which impiles that $a_2 = 4, n = 16$.

Suppose $a_3 = 1, a_5 = 0$, so that $n = 2^{a_2} \cdot 3$. Then $\phi(n) = \phi(2^{a_2} \cdot 3) = 2^{a_2-1}(2-1)3^0(3-1) = 2^{a_2}$. This implies that $a_2 = 3, n = 8 \cdot 3 = 24$.

Suppose $a_3 = 0, a_5 = 1$, so that $n = 2^{a_2} \cdot 5$. Then $\phi(n) = \phi(2^{a_2} \cdot 5) = 2^{a_2-1}(2-1)5^0(5-1) = 2^{a_2+1}$. This implies that $a_2 = 2, n = 4 \cdot 5 = 20$.

Suppose $a_3 = 1, a_5 = 1$, so that $n = 2^{a_2} \cdot 3 \cdot 5$. If $a_2 > 0$ then $\phi(n) = \phi(2^{a_2} \cdot 3 \cdot 5) = 2^{a_2-1}(2-1)3^0(3-1)5^0(5-1) = 2^{a_2+2}$. This implies that $a_2 = 1, n = 2 \cdot 3 \cdot 5 = 30$. If $a_2 = 0$ then instead $\phi(n) = \phi(3 \cdot 5) = 2 \cdot 4 = 8$ does in fact work, so $n = 15$.

Thus the possibilities are $n = 15, 16, 20, 24, 30$.

5.2 Summatory functions

For further reading on the material in this subsection, consult **Rosen 7.2, Shoup 2.9**.

In this section we'll discuss another class of multiplicative functions, known as summatory functions. Though these do not look like they should be multiplicative, they often are.

Definition 5.11. If f is an arithmetic function, we define the *summatory function of f* to be

$$F(n) = \sum_{d|n} f(d)$$

where the sum is over all numbers d which divide n.

Definition 5.12. We define the *number of divisors function* $\tau(n)$ to be the number of natural numbers $\leq n$ which divide n. We can write $\tau(n) = \sum_{d|n} 1$ so τ is a summatory function.

We define the *sum of divisors function* $\sigma(n) = \sum_{d|n} d$ to be the sum of the divisors of n. From the definition we see that σ is also a summatory function.

Proposition 5.13. *If f is a multiplicative function, then the summatory function of f, $F(n) = \sum_{d|n} f(d)$, is also multiplicative.*

This result seems quite surprising at first, since addition and multiplication don't always play well together. Our basic strategy is to write each divisor of mn as a divisor of m times a divisor of n–and this is unique since m and n share no common factors. Thus we can split our sum of divisors of mn into a product of sums of divisors of m and sums of divisors of n.

Proof. Suppose $(m, n) = 1$. We wish to prove that $F(mn) = F(m)F(n)$. We know that $F(mn) = \sum_{d|mn} f(d)$.

We can write any factor of mn uniquely as a product of a factor d_1 of m, and a factor d_2 of n, and we have $(d_1, d_2) = 1$. Thus we have

$$F(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m, d_2|n} f(d_1 d_2) = \sum_{d_1|m, d_2|n} f(d_1)f(d_2).$$

But this sum factors, since we can write

$$\begin{aligned}\sum_{d_1|m, d_2|n} f(d_1)f(d_2) &= \sum_{d_1|m}\sum_{d_2|n} f(d_1)f(d_2) = \sum_{d_1|m}\left(f(d_1)\sum_{d_2|n} f(d_2)\right)\\ &= \left(\sum_{d_1|m} f(d_1)\right)\left(\sum_{d_2|n} f(d_2)\right) = F(m)F(n).\end{aligned}$$

□

Corollary 5.14. *$\sigma(n)$ and $\tau(n)$ are multiplicative functions.*

Lemma 5.15. *Let p be prime and $a \in \mathbb{N}$. Then $\tau(p^a) = a + 1$ and*

$$\sigma(p^a) = 1 + p + p^2 + \cdots + p^a = \frac{p^{a+1} - 1}{p - 1}.$$

Proof. The divisors of p^a are $1, p, p^2, \ldots, p^a$. Thus there are $a+1$ and the result for τ follows. The first formula for σ also follows; the second comes from the geometric series formula, or from the difference of $a + 1$st powers formula. □

Corollary 5.16. *Let $n = \prod_{i=1}^k p_i^{a_i}$. Then*

$$\sigma(n) = \prod_{i=1}^k \frac{p_i^{a_i+1} - 1}{p_i - 1}$$
$$\tau(n) \prod_{i=1}^k (a_i + 1).$$

Theorem 5.17. *Let n be a positive integer. Then $\sum_{d|n} \phi(d) = n$. That is, the summatory function of the Euler ϕ-function is the identity function.*

Proof. We're going to turn this into a counting/combinatorial argument. We're going to divide the integers $\leq n$ into classes C_d, where each class will contain exactly one number d which divides n, and the class will have $\phi(n/d)$ elements. Thus $\sum_{d|n} \phi(n/d) = \sum_{d|n} \#C_d$, and the latter sum must be n since it sums the sizes of a collection of sets whose union is $\{1, \ldots, n\}$.

Say the integer m is in the class C_d if $1 \leq m \leq n$ and $(m, n) = d$. We see that $m|n$ if and only if $(m, n) = m$, so C_d contains exactly one element, d, which divides n.

Further, we see that $m \in C_d$ if and only if $(m, n) = d$, which happens if and only if $(m/d, n/d) = 1$. Thus the number of integers in C_d is the number of integers $\leq n/d$ which are relatively prime to n/d–that is, the size of C_d is $\phi(n/d)$. And this proves what we wanted. □

5.3 Perfect Numbers and Mersenne Primes

For further reading on the material in this subsection, consult **Rosen 7.3, Wikipedia**.

Definition 5.18. We say a positive integer n is a *perfect number* if $\sigma(n) = 2n$.

Example 5.19. Famously 6 is perfect, since $\sigma(6) = 1 + 2 + 3 + 6 = 12$.

28 is perfect since $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56$.

Theorem 5.20. *The positive even integer n is perfect if and only if $n = 2^{m-1}(2^m - 1)$ where $m \geq 2$ and $2^m - 1$ is prime.*

Proof. First we show that if $2^m - 1$ is prime then $n = 2^{m-1}(2^m - 1)$ is perfect. Because σ is multiplicative and we have a formula for it, we have

$$\begin{aligned}\sigma(n) &= \sigma(2^{m-1}(2^m - 1)) = \sigma(2^{m-1})\sigma(2^m - 1) \\ &= \frac{2^m - 1}{2 - 1} \cdot (1 + 2^m - 1) = (2^m - 1)2^m = 2n.\end{aligned}$$

Now we want to show that if $\sigma(n) = 2n$ and n is even, then $n = 2^{m-1}(2^m - 1)$ for some m. So write $n = 2^s t$ where t is odd. Then

$$\sigma(n) = \sigma(2^s)\sigma(t) = \frac{2^{s+1}-1}{2-1} \cdot \sigma(t) = (2^{s+1}-1)\sigma(t).$$

But since n is perfect, we know $\sigma(n) = 2n = 2^{s+1}t$ and thus we have

$$2^{s+1}t = (2^{s+1}-1)\sigma(t)$$

and thus 2^{s+1} divides $(2^{s+1}-1)\sigma(t)$.

But we can see that $(2^{s+1}, 2^{s+1}-1) = 1$, so by Euclid's Lemma $2^{s+1}|\sigma(t)$. So let $\sigma(t) = 2^{s+1}q$ for some integer q, and we have

$$\begin{aligned} 2^{s+1}t &= (2^{s+1}-1)2^{s+1}q \\ t &= (2^{s+1}-1)q = 2^{s+1}q - q. \end{aligned}$$

Thus $q|t$ and $q \neq t$.

Adding q to both sides gives $t + q = 2^{s+1}q = \sigma(t)$. But if $q > 1$ then, since $q|t$ and $q \neq t$, we have (at least) three distinct positive divisors of t: $1, q$, and t. Thus $1 + q + t \leq \sigma(t) = q + t$ which is a contradiction. Thus $q = 1$, and $\sigma(t) = t + 1$. But if $\sigma(t) = t + 1$ this implies the only positive factors of t are 1 and t, and thus by definition t is prime. Further $t = (2^{s+1}-1)q = 2^{s+1} - 1$. □

Thus to find all (even) perfect numbers, we just need to find primes of the form $2^m - 1$. This brings us to a famous old category of primes, called the Mersenne primes.

Definition 5.21. If $m \in \mathbb{N}$, then $M_m = 2^m - 1$ is called the *mth Mersenne number*. If M_m is prime, it is called a Mersenne prime.

Proposition 5.22. *If $m \in \mathbb{N}$ and $M_m = 2^m - 1$ is prime, then m is prime.*

Suppose $m = ab$ for $1 < a, b < m$. Then

$$2^m - 1 = 2^{ab} - 1 = (2^a - 1)(1 + 2^a + 2^{2a} + \cdots + 2^{(b-2)a} + 2^{(b-1)a}).$$

Since $a, b > 1$, both of these factors are > 1, so $2^m - 1$ is not prime, which is a contradiction.

Remark 5.23. Note that it is *not* true that if p is prime, then M_p is as well. The smallest "pernicious Mersenne number"–that is, M_p where p is prime but M_p is not– is $M_{11} = 2^{11} - 1 = 2047$, which we have discussed in class before.

Mersenne primes provide a relatively easy way to find large primes; the largest known prime is $2^{74,207,281}-1$, which is a Mersenne prime. The GIMPS (Great Internet Mersenne Prime Search) is a large distributed computing project to test larger candidate Mersenne primes.

It was for a long time inaccurately believed that M_{67} was prime (after Marin Mersenne wrongly included it on his list of Mersenne primes in the 17th century; he also wrongly included M_{257} and excluded M_{61}, M_{89}, and M_{107}. Edouard Lucas showed in 1876 that M_{67} was composite, but did not find a factor.

In 1903, Frank Nelson Cole gave a completely silent "talk" in which he computed $2^{67}-1$ and $193,707,721 \times 761,838,257,287$ on the blackboard and got the same number both ways (a result which he said took him "three years of Sundays" to find). He returned to his seat without speaking, to applause from the audience.

Though M_p is not always prime for p prime, we have a number of theorems that will help us decide of M_p is in fact prime.

Theorem 5.24. *If p is an odd prime, then any divisor of $M_p = 2^p - 1$ is of the form $2kp+1$ where $k \in \mathbb{N}$.*

Proof. Let q be a prime dividing $M_p = 2^p - 1$. By Fermat's little theorem we know that $2^{q-1} \equiv 1 \mod q$ and thus $q|2^{q-1}-1$. We can compute that $(2^p-1, 2^{q-1}-1) = 2^{(p,q-1)}-1$. But since $q|2^p-1, 2^{q-1}-1$, we know that $q|2^{(p,q-1)}-1$ and thus $(p, q-1) > 1$. But p is prime, so $(p, q-1) = p$.

Thus $p|q-1$ so there is a natural number m such that $mp = q-1$. Since q, p are odd, we know that m is even, so write $m = 2k$ for $k \in \mathbb{N}$. Thus $q = 2kp+1$, and any prime divisor of M_p has the form $2kp+1$. But the product of two numbers of this form is still a number of this form, and any divisor of M_p is the product of prime divisors, so any divisor has the form $2kp+1$. □

Corollary 5.25. *There are infinitely many primes.*

Proof. Suppose there are finitely many primes, and let p be the largest. Then $M_p > p$ is not prime, and it has some prime factor. But by theorem 5.24, the prime factor must have the form $2kp+1 > p$, which is a contradiction. □

Example 5.26. Let us decide whether $M_{13} = 2^{13}-1 = 8191$ is prime. We only need to check for factors less than $\sqrt{8191} \approx 90$. Further, any factor must have the form $2 \cdot k \cdot 13 + = 26k+1$, so we just have to check $27, 53, 79$. 27 isn't prime so we just need to check 53 and 79. But $8191/53 = 154.547$ and $8191/79 = 103.684$. Thus M_{13} must be prime.

Now let's decide if $M_{23} = 2^{23} - 1 = 8,388,607$ is prime. We only need to check primes of the form $46k + 1$. The first of these is 47, and we see $8,388,607/47 = 178,481$. Thus M_{23} is not prime.

Remark 5.27. There is a more efficient test to determine whether a Mersenne number is prime, called the *Lucas-Lehmer Test*. This could make a good paper topic for someone familiar with group theory.

Two last comments on this topic: first, all our work on Mersenne primes was specific to the base 2. We can't actually extend this work to other bases. Or rather, we can, but it's very brief.

Exercise 5.28. *Suppose $a^p - 1$ is prime. Then either $a \leq 2$ or $p = 1$.*

Second, we've only addressed even perfect numbers. It's actually an open question whether odd perfect numbers exist, and commonly conjectured that they do not. We do know a large number of conditions that odd perfet numbers must satisfy:

Fact 5.29. *Suppose N is an odd perfect number. Then*

- *N is not divisible by 105*
- *N satisfies one of $N \equiv 1 \mod 12$, $N \equiv 117 \mod 468$, or $N \equiv 81 \mod 324$*
- *$N = q^a p_1^{2e_1} \dots p_k^{2e_k}$ where*
  - *$q, p_1, \dots, p_k$ are distinct primes*
  - *$q \equiv a \equiv 1 \mod 4$*
  - *The smallest prime factor of N is less than $(2k + 8)/3$*
  - *Either $q^a > 10^{62}$, or $p_j^{2e_j} > 10^{62}$ for some j*
  - *$N < 2^{4^{k+1}}$*
- *The largest prime factor of N is greater than 10^8, the second largest prime factor is greater than 10^4, and the third largest is greater than 100*
- *N has at least 101 prime factors and at least 10 distinct prime factors, and if $3 \nmid N$ then N has at least 12 distincct prime factors.*

- $N > 10^{1500}$

This list of restrictions is sufficiently long that James Joseph Sylvester commented in 1888 that: "...a prolonged meditation on the subject has satisfied me that the existence of any one such [odd perfect number] its escape, so to say, from the complex web of conditions which hem it in on all sides would be little short of a miracle."

5.4 Mobius Inversion

We earlier discussed summatory functions, where we write $F(n) = \sum_{d|n} f(n)$ for some function f; we proved that if f is multiplicative, then so is F. In this section we'd like to reverse the summatory function process. That is, if we have $F(n)$ can we use that to compute $f(n)$?

Well, we'll start by exploring. We notice that

$$\begin{aligned}
F(1) &= f(1) \\
F(2) &= f(1) + f(2) \\
F(3) &= f(1) + f(3) \\
F(4) &= f(1) + f(2) + f(4) \\
F(5) &= f(1) + f(5) \\
F(6) &= f(1) + f(2) + f(3) + f(6)
\end{aligned}$$

and thus

$$\begin{aligned}
f(1) &= F(1) \\
f(2) &= F(2) - f(1) = F(2) - F(1) \\
f(3) &= F(3) - f(1) = F(3) - F(1) \\
f(4) &= F(4) - f(2) - f(1) = F(4) - (F(2) - F(1)) - F(1) \\
&= F(4) - F(2) \\
f(5) &= F(5) - f(1) = F(5) - F(1) \\
f(6) &= F(6) - f(3) - f(2) - f(1) = F(6) - (F(3) - F(1)) - (F(2) - F(1)) - F(1) \\
&= F(6) - F(3) - F(2) + F(1).
\end{aligned}$$

We might notice that we seem to always be able to write $f(n)$ as a sum of $\pm F(n/d)$ for $d|n$. So we might hope we can find an arithmetic function μ that gives a formula

$$f(n) = \sum_{d|n} \mu(d) F(n/d).$$

Let's figure out what this function would have to look like. $f(1) = F(1)$ so $\mu(1) = 1$. If p is a prime, then $F(p) = f(1) + f(p)$ so $f(p) = F(p) - F(1)$. Thus we must have $\mu(p) = -1$. (Recall that we have $\mu(d)F(n/d)$ so $\mu(p)$ is the coefficient of $F(1)$).

By the same logic, we see that $F(p^2) = f(1) + f(p) + f(p^2)$ so $f(p^2) = F(p^2) - F(p)$. Thus if $\mu(1) = 1$ and $\mu(p) = -1$, we have $\mu(p^2) = 0$. We can follow the same argument to show that $\mu(p^k) = 0$ for every $k > 1$.

If we assume that μ is multiplicative, this completely nails down the values of μ at every number, since we can "compute" it at any prime power. This leads us to the following definition:

Definition 5.30. We define the *Möbius function* $\mu(n)$ by

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^r & n = p_1 p_2 \dots p_r \text{ are distinct primes} \\ 0 & \text{otherwise} \end{cases}$$

In particular, if $p^2 | n$ for any prime p then $\mu(n) = 0$. $\mu(n) \neq 0$ if and only if n is *square-free*.

Remark 5.31. If we think of 1 as the empty product, then we don't need to define $\mu(1)$ separately, since $1 = \prod_{k=1}^{0} p_i$ and then $\mu(1) = (-1)^0$.

Example 5.32.

$$\begin{aligned} \mu(1) &= 1 & \mu(4) &= 0 \\ \mu(2) &= -1 & \mu(5) &= -1 \\ \mu(3) &= -1 & \mu(6) &= 1. \end{aligned}$$

We can compute that

$$\begin{aligned} \mu(330) &= \mu(2 \cdot 3 \cdot 5 \cdot 11) = (-1)^4 = 1 \\ \mu(660) &= \mu(2^2 \cdot 3 \cdot 5 \cdot 11) = 0 \\ \mu(2310) &= \mu(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11) = (-1)^5 = -1. \end{aligned}$$

Lemma 5.33. *The Möbius function $\mu(n)$ is multiplicative.*

Proof. Suppose m, n are relatively prime positive integers. We want to show that $\mu(mn) = \mu(m)\mu(n)$. We need to check this case-by-case.

If $m = 1$ then $\mu(m) = 1$, so $\mu(mn) = \mu(n) = \mu(m)\mu(n)$. Similarly if $n = 1$ then $\mu(mn) = \mu(m) = \mu(m)\mu(n)$.

If m is divisible by a square of a prime, then so is mn, so $\mu(mn) = 0 = 0{\cdot}\mu(n) = \mu(m)\mu(n)$. Similarly, if n is divisible by a square of a prime, then so is mn, so $\mu(mn) = 0 = \mu(m) \cdot 0 = \mu(m)\mu(n)$.

Finally, suppose $m, n \neq 1$ and neither is divisible by a square of a prime. Then we we can write $m = p_1 \dots p_k$ and $n = q_1, \dots, q_\ell$ where the p_i and the q_i are all distinct. Then we have $\mu(m) = (-1)^k, \mu(n) = (-1)^\ell$. We also have $mn = p_1 \dots p_k q_1 \dots q_\ell$ all distinct factors, so $\mu(mn) = (-1)^{k+\ell} = (-1)^k(-1)^\ell = \mu(m)\mu(n)$. □

Remark 5.34. The Möbius function is not completely multiplicative, since $\mu(2) = -1$ but $\mu(4) = 0$.

Since we have a multiplicative function, the next step is to study its summatory function. Fortunately, the Möbius function has a particularly simple summatory function:

Lemma 5.35. *The summatory function of the Möbius function satisfies the formula*

$$F(n) = \sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 1. \end{cases}$$

Proof. When $n = 1$, we have $F(1) = \sum_{d|1} \mu(d) = \mu(1) = 1$.

Now suppose $n > 1$. We know that F is multiplicative, so we just need to evaluate it at prime powers. But

$$\begin{aligned} F(p^k) &= \sum_{d|p^k} \mu(d) = \mu(1) + \mu(p) + \dots + \mu(p^k) \\ &= 1 - 1 + 0 + 0 + \dots + 0 = 0 \end{aligned}$$

as long as $k > 0$.

Suppose $n = p_1^{a_1} \dots p_k^{a_k}$. Then

$$F(n) = \prod_{i=1}^k F(p_i^{a_i}) = \prod_{i=1}^k 0 = 0.$$

□

So far we've studied some properties of our Möbius function, but we haven't actually proven that it does the thing we want it to do. Recall we were hoping to find an "inversion formula" that allows us to recapture a function from its summative function. If such a function exists and is multiplicative, it must be the Möbius function; but now we're ready to prove that the Möbius function does in fact have this property.

Theorem 5.36 (Möbius Invrsion Formula)**.** *Suppose f is an arithmetic function (which need not be multiplicative!), and F is the summatory function of f, given by*

$$F(n) = \sum_{d|n} f(d).$$

Then, for any natural number n, we have

$$f(n) = \sum_{d|n} \mu(d) F(n/d).$$

Proof. The proof of this is a fairly straightforward exercise in manipulation of sums, but we must be careful of our indices.

Fix an integer n. We have

$$\begin{aligned}\sum_{d|n} \mu(d) F(n/d) &= \sum_{d|n} \left(\mu(d) \sum_{e|(n/d)} f(e) \right) \\ &= \sum_{d|n} \sum_{e|(n/d)} \mu(d) f(e).\end{aligned}$$

Now we think about the indices. We're summing over all pairs of integers d, e such that $d|n$ and $e|n/d$. But this is the same as summing over all pairs of integers d, e such that $e|n$ and $d|(n/e)$. (Suppose $d|n$ and $em = n/d$. Then $emd = n$ so $e|n$, and $md = n/e$ so $d|n/e$. We can do the same argument in the opposite direction). Thus we have

$$\begin{aligned}\sum_{d|n} \sum_{e|(n/d)} \mu(d) f(e) &= \sum_{e|n} \sum_{d|(n/e)} \mu(d) f(e) \\ &= \sum_{e|n} f(e) \left(\sum_{d|(n/e)} \mu(d) \right).\end{aligned}$$

But recall that $\sum_{d|(n/e)} \mu(d) = 0$ unless $n/e = 1$, which happens precisely when $e = n$, and in this case the sum is equal to 1. So every term of this sum is 0 except the term corresponding to $e = n$, which gives us

$$\sum_{e|n} f(e) \sum_{d|(n/e)} \mu(d) = f(e) \cdot 1 = f(e).$$

□

This is all an example of a process called *Dirichlet convolution*, which you will see more about on the homework.

Corollary 5.37. *If n is a natural number, we have*

$$n = \sum_{d|n} \mu(d)\sigma(n/d) = \sum_{d|n} \mu(n/d)\sigma(d)$$
$$1 = \sum_{d|n} \mu(d)\tau(n/d) = \sum_{d|n} \mu(n/d)\tau(d).$$

Corollary 5.38. *Let f be an arithmetic function and $F(n) = \sum_{d|n} f(n)$ be the summatory function of f. If F is multiplicative, then so is f.*

Remark 5.39. Notice this is the converse of proposition 5.13, which said that if f is multiplicative, then so is its summatory function.

Proof. Suppose m, n are relatively prime natural numbers. We want to show that $f(mn) = f(m)f(n)$. First recall that if $d|mn$ then we can uniquely write $d = d_1d_2$ with $d_1|m, d_2|n$ (since m, n share no factors in common), and $(d_1, d_2) = 1$. Then

$$\begin{aligned} f(mn) &= \sum_{d|mn} \mu(d)F\left(\frac{mn}{d}\right) \\ &= \sum_{d_1|m, d_2|n} \mu(d_1d_2)F\left(\frac{mn}{d_1d_2}\right) \\ &= \sum_{d_1|m, d_2|n} \mu(d_1)\mu(d_2)F\left(\frac{m}{d_1}\right)\left(\frac{n}{d_2}\right) \\ &= \left(\sum_{d_1|m} \mu(d_1)F(m/d_1)\right)\left(\sum_{d_2|n} \mu(d_2)F(n/d_2)\right) \\ &= f(m)f(n). \end{aligned}$$

□