Math 313/623 Notes 6

David L. Meretzky

Tuesday March 12th, 2019

> Seven point six two, five point five six's, two-two-three
>
> YNW Melly

In these notes we will investigate some important arithmetic functions and the Möbius transformation.

Applications of Unique Factorization

Some Arithmetic Functions

Definition 1. Let $a \in \mathbb{Z}$ is square-free if it is not divisible by the square of any other integer greater than 1.

In particular a number is square free if and only if it is the product of distinct primes.

Proposition 1. If $n \in \mathbb{Z}$ n can be written in the form $n = ab^2$ where $a, b \in \mathbb{Z}$ and a is square-free.

Example 1. Let $n = 2^3 \cdot 3^3$. In this case, n can be rewritten as $(2 \cdot 3) \cdot (2 \cdot 3)^2$ where $a = 2 \cdot 3$ and $b = 2 \cdot 3$.

Proof. We may factor n into primes $n = p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$. Furthermore, each exponent can be written in the form, $a_i = 2b_i + r_i$ with $r_i = 0$ or $r_i = 1$ depending on whether or not each exponent is even or odd. Then set $a = p_1^{r_1} p_2^{r_2} \cdots p_l^{r_l}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_l^{b_l}$. Then

$$n = p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l} = p_1^{2b_1 + r_1} p_2^{2b_2 + r_2} \cdots p_l^{2b_l + r_l} = (p_1^{r_1} p_2^{r_2} \cdots p_l^{r_l})(p_1^{b_1} p_2^{b_2} \cdots p_l^{b_l})^2 = ab^2$$

as desired. □

We can use this new representation to obtain a second proof that there are infinitely many primes in the integers.

Theorem 1. There are infinitely many primes in $\mathbb{Z}$.

Proof. Assume there are only finitely many primes $p_1, \ldots, p_l$. Consider the set of positive integers less than or equal to an arbitrary number N. If $n \leq N$, represent n as $n = ab^2$ where a is square free. Since there are only l primes,

there are only 2^l ways of picking distinct primes from the list of primes. That is, $a = p_1^{\varepsilon_1} \cdots p_l^{\varepsilon_l}$ where ε_i is either 0 or 1. There are 2^l possible choices for a. Note also that $b \leq \sqrt{N}$ because otherwise $n = ab^2 \geq N$. Each number $n \leq N$ is specified by picking a choice of a and a choice of b. Since there are 2^l ways to choose a and $\sqrt{N}$ ways to choose b, the total possible number of choices of numbers less than N is at the most $2^l\sqrt{N}$.

Thus $N \leq 2^l\sqrt{N}$ the number of numbers less than or equal to N, which is N, must be less than the minimum number of ways of expressing a number as ab^2 because otherwise there would be numbers less than N which could not be expressed as ab^2.

However, $N \leq 2^l\sqrt{N}$ implies (by dividing both sides by $\sqrt{N}$) $\sqrt{N} \leq 2^l$ which we can make false by just picking a large enough N. Thus there cannot possibly be only finitely many primes. □

Now we will define some number theoretic functions.

Definition 2. For $n \in \mathbb{Z}$ let $v(n)$ denote the number of positive divisors of n.

Proposition 2. Given $n \in \mathbb{Z}$ with prime factorization $n = p_1^{a_1} \cdots p_l^{a_l}$, then $v(n) = (a_1 + 1) \cdots (a_l + 1)$.

Proof. Every divisor of n is of the form $p_1^{b_1} \cdots p_l^{b_l}$ where for each $i \in \{1, \ldots, l\}$ we have $0 \leq b_i \leq a_i$. Thus each b_i could be any one of the $a_i + 1$ possible numbers between 0 and a_i. Since each divisor is determined by picking each b_i, and there are $(a_i + 1)$ ways to pick each b_i, the total number of possible divisors is the product $(a_1 + 1) \cdots (a_l + 1)$. □

Example 2. Let p be a prime, then $v(p) = 2$.

Take a moment to compute v for various numbers. Make sure to convince yourself that the formula $v(n) = (a_1 + 1) \cdots (a_l + 1)$ works.

Definition 3. For $n \in \mathbb{Z}$ let $\sigma(n)$ denote the sum of the positive divisors of n.

Example 3. For instance, for a prime p, $\sigma(p) = p + 1$.

Proposition 3. Given $n \in \mathbb{Z}$ with prime factorization $n = p_1^{a_1} \ldots p_l^{a_l}$, then

$$\sigma(n) = \left(\frac{p_1^{a_1+1} - 1}{p_1 - 1}\right) \cdots \left(\frac{p_l^{a_1+1} - 1}{p_l - 1}\right)$$

.

Proof. By definition,

$$\sigma(n) = \sum_{b_1=0}^{a_1} \cdots \sum_{b_l=0}^{a_l} p_1^{b_1} \cdots p_l^{b_l} = \left(\sum_{b_1=0}^{a_1} p_1^{b_1}\right) \cdots \left(\sum_{b_l=0}^{a_l} p_l^{b_l}\right)$$

By the formula for geometric series in the finite case, we have

$$\left(\sum_{b_1=0}^{a_1} p_1^{b_1}\right)\cdots\left(\sum_{b_l=0}^{a_l} p_l^{b_l}\right) = \left(\frac{p_1^{a_1+1}-1}{p_1-1}\right)\cdots\left(\frac{p_l^{a_1+1}-1}{p_l-1}\right)$$

as desired. □

Definition 4. We call a number n perfect if $\sigma(n) = 2n$. For example, 6 and 28 are perfect.

Exercise 1. It is delightfully satisfying to show that if $2^{m+1}-1$ is prime (such primes are called mersenne primes) then $n = 2^m(2^{m+1}-1)$ is perfect. This is not hard, you simply apply the proposition and compute. Euclid knew this fact. Euler showed any perfect number is of this form. It is not known if there are infinitely many perfect numbers or if there are any odd perfect numbers.

We will now define one of the most important number theoretic functions. It is called the Möbius μ function. Roughly, it measures whether the number of primes appearing in a prime factorization is even or odd. Recall that every square-free number has prime a factorization which is a distinct product of primes, that is, no prime appears with a power greater than 1. so if a is square free, $a = p_1 \cdots p_l$, for distinct primes $p_1, \ldots, p_l$.

Definition 5. For $n \in \mathbb{Z}^+$, we define the Möbius μ function by setting $\mu(1) = 1$, $\mu(n) = 0$ if n is not square-free, and in the case n is square free, $n = p_1 p_2 \cdots p_l$, $\mu(n) = \mu(p_1 p_2 \cdots p_l) = (-1)^l$.

Proposition 4. If $n > 1$, then

$$\sum_{d|n} \mu(d) = 0$$

Before looking at the following proof. Compute by hand the following example: $n = 2^3 3^4 7^2$.

Proof. If $n = p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$ then $\sum_{d|n} \mu(d) = \sum_{(} \epsilon_1, \ldots, \epsilon_l)\mu(p_1^{\epsilon_1} \cdots p_l^{epsilon_l})$, where the ϵ_i are 0 or 1. This is because each divisor must be square-free to be non-zero in the sum. This is the sum over all square-free divisors. Evaluation of the μ function only counts the number of primes in the factorization of each square-free divisor. Thus,

$$\sum_{d|n} \mu(d) = (-1)^0\binom{l}{0} + (-1)^1\binom{l}{1} + (-1)^2\binom{l}{2} + \cdots + (-1)^{l+1}\binom{l}{l} = 0$$

For instance, if there are k primes in a divisor where k, the contribution of that divisor in the sum is $(-1)^k$. Furthermore, there are exactly $\binom{l}{k}$ ways to create a square-free divisor of n, with k primes. Thus the contribution of the divisors with k primes in the sum is $(-1)^k\binom{l}{k}$. □

Definition 6. Let f and g be functions from $\mathbb{Z}^+$ into $\mathbb{C}$, the complex numbers. The Dirichlet product of f and g is denoted $f \circ g$ and is defined as follows. For $n \in \mathbb{Z}^+$, $(f \circ g)(n) = \sum f(d_1)g(d_2)$ where the sum is over all products (d_1, d_2) such that $d_1 d_2 = n$.

A notational aside: We write the Dirchlet product of f and g, $f \circ g$, evaluated at n as $f \circ g(n)$ not as $(f \circ g)(n)$ to avoid using tons of parentheses. Note that $f \circ g(n)$ does not mean the dirichlet product of f and $g(n)$, which is not defined, it means the dirichlet product of f and g, $f \circ g$, evaluated at n.

Exercise 2. Compute the dirichlet product of $f(n) = n$ and $g(n) = n^2$, $f \circ g(6)$.

Proposition 5. The Dirichlet product is associative, meaning $f \circ (g \circ h) = (f \circ g) \circ h$. It is also commutative.

Proof. Exercise. Check that when evaluated at some n, both sides of the equality are equal to

$$\sum_{(d_1,d_2,d_3)} f(d_1)g(d_2)h(d_3)$$

where the sum is over all triples (d_1, d_2, d_3), such that $d_1 d_2 d_3 = n$. Prove also that it is commutative. This is easy. □

Definition 7. Define the function $\mathbb{I}$ as follows: $\mathbb{I}(1) = 1$, $\mathbb{I}(n) = 0$ for $n > 0$.

Proposition 6. The Dirichlet product $f \circ \mathbb{I} = \mathbb{I} \circ f = f$.

Proof. Compute

$$f \circ \mathbb{I}(n) = \sum_{(d_1,d_2)} f(d_1)\mathbb{I}(d_2) = 0 + 0 + \cdots + 0 + f(n)\mathbb{I}(1) = f(n)$$

that is the only term that survives in the sum is when $d_2 = 1$, otherwise $\mathbb{I}$ will kill the second factor. Compute $\mathbb{I} \circ f(n)$ analogously. □

Definition 8. Define the function I as follows, $I(n) = 1$ for all $n \in \mathbb{Z}^+$.

Proposition 7. The Dirichlet product $I \circ f(n) = f \circ I(n) = \sum_{d|n} f(d)$

Proof. Compute $I \circ f(n) = \sum_{(d_1,d_2)} I(d_1)f(d_2) = \sum_{(d_1,d_2)} f(d_2) = \sum_{d|n} f(d)$. The last equality holds because d_2 is going over all numbers such that there exists a d_1 such that $d_1 d_2 = n$. This is exactly the set of d which divide n. Compute $f \circ I(n)$ analogously. □

Lemma 1. The Dirichlet product, $I \circ \mu = \mu \circ I = \mathbb{I}$.

Proof. For $n = 1$, $I \circ \mu(n) = I(1)\mu(1) = 1(1) = 1$. For $n > 1$, $I \circ \mu(n) = \sum_{d|n} \mu(d) = 0$ by propositions 7 and 4. □

Theorem 2. Möbius Inversion Formula: Let $F(n) = \sum_{d|n} f(d)$, then $f(n) = \sum_{d|n} \mu(d)F(n/d)$.

Proof. $F(n) = f \circ I$. Thus $F \circ \mu = (f \circ I) \circ \mu = f \circ (I \circ \mu) = f \circ \mathbb{I} = f$. Thus,

$$f(n) = F \circ \mu(n) = \sum_{(d_1,d_2)} \mu(d_1)F(d_2) = \sum_{d|n} \mu(d)F(n/d)$$

since $d_1 d_2 = n$. □

We will see an application of the Möbius Inversion Formula to end these notes.

Definition 9. (Euler ϕ function)[1]For $n \in \mathbb{Z}^+$, $\phi(n)$ is defined to be the number of integers k, $1 \leq k \leq n$, such that k is relatively prime to n, meaning $(k, n) = 1$.

Example 4. For instance, $\phi(1) = 1$, $\phi(5) = 4$, $\phi(6) = 2$, and in general for a prime p, $\phi(p) = p - 1$.

Proposition 8. $\sum_{d|n} \phi(d) = n$.

Proof. Consider the n rational numbers $\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n}$. Reduce each fraction to lowest terms. Then the numerator and denominator will be relatively prime. Claim: if $d|n$ then exactly $\phi(d)$ of the denominators will be d. Since the claim is true (you will show this in an exercise; we also did this in class), and since every denominator will be a divisor of n it follows that $\sum_{d|n} \phi(d) = n$. □

Proposition 9. Let $n \in \mathbb{Z}^+$ with prime factorization $n = p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$. Then

$$\phi(n) = n(1 - (1/p_1))(1 - (1/p_2)) \cdots (1 - (1/p_l)).$$

Proof. Since $n = \sum_{d|n} \phi(d)$, applying the Möbius Inversion Formula, we obtain $\phi(n) = \sum_{d|n} \mu(d)(n/d)$ and by the definition of μ we see that the only divisors which survive are the square free divisors, that is the d which are a product of distinct primes. Additionally, the parity[2] of the number of distinct primes, determines if $\mu(d) = \pm 1$. For instance if d is composed of 1 prime then $\mu(d) = (-1)^1$. Expanding the sum we obtain

$$\phi(n) = n + \sum_i (-1)^1 (n/p_i) + \sum_{i<j} (-1)^2 (n/p_i p_j) + \sum_{i<j<k} (-1)^3 (n/p_i p_j p_k) + \cdots$$

where each sum is over the possible ways of picking r distinct primes out of l. This is the same as the ways of picking r increasing indicies $i_1 < i_2 < \cdots < i_r$ where each i_s is one of $1, 2, \ldots, l$.

[1] ϕ is pronounced "fai", rhyming with "eye", and written in english: phi. It's all greek to me too, don't worry.

[2] evenness or oddness

By inspection we see that

$$n - \sum_i (n/p_i) + \sum_{i<j} (n/p_i p_j) - \cdots = n(1-(1/p_1))(1-(1/p_2))\cdots(1-(1/p_l)).$$

□

Exercises

1. Show that if $2^{m+1}-1$ is prime, then $n = 2^m(2^{m+1}-1)$ is perfect.
2. Prove that for any positive integer l,

$$(-1)^0\binom{l}{0} + (-1)^1\binom{l}{1} + (-1)^2\binom{l}{2} + \cdots + (-1)^{l+1}\binom{l}{l} = 0.$$

   Hint: split this into two cases, l is even and l is odd.
3. Prove the claim in the proof of proposition 8.
4. Compute $\phi(2^5)$
5. Compute $\phi(3^4)$
6. Compute $\phi(7^{10})$
7. Prove that $\phi(p^k) = p^k - p^{k-1}$ where p is prime.
8. Give the alternate proof of proposition 8 that we did in class using the previous exercise, the fact that $\phi(mn) = \phi(m)\phi(n)$ where $(m,n) = 1$, and unique factorization.