CS 70 Discrete Mathematics and Probability Theory
Summer 2019 Course Notes

Bonus Note 2

1 Euler's Totient Theorem

In note 6.5, we proved Fermat's Little Theorem: that if a was not divisible by a prime p, a^{p-1} would be 1 modulo p. While this is highly useful for many applications, as seen in note 7, the constraint that p is a prime can be somewhat of a hindrance; we would ideally like to be able to state a version of FLT which does not require a prime modulus. This is precisely what Euler's Totient Theorem does.

Before giving the formal statement of the theorem, let's first think about what would happen if we tried to prove FLT exactly as we did in note 6, except that our modulus is no longer prime. The proof can roughly be broken down into the following steps:

(1) Define the set $S = \{1, 2, ..., p-1\}$

(2) The function $f(x) = ax \bmod p$ is a bijection from S to itself.

(3) Hence $\prod_{i \in S} i = \prod_{i \in S} (ai \bmod p) \equiv a^{p-1} \prod_{i \in S} i \pmod{p}$

(4) Each $i \in S$ has an inverse modulo p, so $(\prod_{i \in S} i)^{-1} \equiv \prod_{i \in S} (i^{-1}) \pmod{p}$ exists.

(5) Multiply both sides of step 3 by this inverse to get $a^{p-1} \equiv 1 \pmod{p}$

If we replace p with some composite modulus m, step 2 will immediately fail. Just knowing that a is not divisible by m is not sufficient to conclude that $f(x)$ will be a bijection from S to itself. Indeed, if we consider $m = 4$ and $a = 2$, our set S will be $\{1, 2, 3\}$, but if we apply f to each element, we'll get $f(1) = 2$, $f(2) = 0$, and $f(3) = 2$. In this case, f is not even a function from S to itself, much less a bijection!

In order to get around this problem, we will specify not only that $a \not\equiv 0 \pmod{m}$, but more strongly that $\gcd(a, m) = 1$.[1] With this fix, step 2 will go by without a hitch, as a being coprime to m gives us an inverse for a mod m, allowing us to define an inverse function $f^{-1}(y) = a^{-1}y \bmod m$.

However, we will now have that step 4 will fail. When we had a prime modulus, we could say that every positive number smaller than it (ie, every element of S) must be coprime to it, but this is not the case with a composite number. Thus, there will be some element of S which is not invertible, meaning that we cannot take the inverse of $\prod_{i \in S} i$.

The fix for this is simple: in step 1, we simply define S to be the set of all numbers smaller than m which are coprime to m. This will ensure that they all have the inverses needed for step 4. With these fixes in place, we can now state and prove Euler's Totient Theorem.

Theorem B2.1 (Euler's Totient Theorem)**.** *Let $\phi(m)$ be the number of positive integers smaller than m that are coprime to m; that is $\phi(m) = |\{x \in \mathbb{Z}_m | \gcd(x, m) = 1\}|$. Then for any a such that $\gcd(a, m) = 1$, we have that $a^{\phi(m)} \equiv 1 \pmod{m}$.*

[1] Do you see why these two were equivalent when our modulus was a prime?

Proof. We start by defining the set $S = \{x \in \mathbb{Z}_m | \gcd(x,m) = 1\}$. We have that the function $f(x) = ax \bmod m$ is a bijection from S to itself. First off, if $\gcd(x,m) = \gcd(a,m) = 1$, we will have that $\gcd(ax,m) = 1$; in other words, if $x \in S$, $f(x) \in S$ as well. Thus, f is indeed a function from S to S as desired. In order to prove that f is a bijection, we note that because $\gcd(a,m) = 1$, a has an inverse mod m, and thus we can define $f^{-1}(y) = a^{-1}y \bmod m$. Since f has an inverse function, we know that it must be a bijection.

Since we know that S is the same set as $\{f(x)|x \in S\}$ (just potentially written in a different order), we must have that the product of the elements in each set is the same. Writing this out mathematically, we have

$$\prod_{i \in S} i = \prod_{i \in S} f(i) = \prod_{i \in S} ai \bmod m \tag{1}$$

As in the proof of Fermat's Little Theorem, we know that it doesn't matter if we take the modulus at intermediate steps or at the end. Thus, we have

$$\prod_{i \in S} ai \bmod m \equiv \prod_{i \in S} ai \equiv a^{|S|} \prod_{i \in S} i \pmod{m} \tag{2}$$

Putting together (1) and (2), and noting that $|S| = \phi(m)$ by definition, we have that

$$a^{\phi(m)} \prod_{i \in S} i \equiv \prod_{i \in S} i \pmod{m} \tag{3}$$

Thus, it only remains to prove that $\prod_{i \in S} i$ has an inverse modulo m. But we note that each $i \in S$ is relatively prime to m, and thus $i^{-1} \pmod{m}$ exists. Hence, since $(\prod_{i \in S} i)^{-1} \equiv \prod_{i \in S} i^{-1} \pmod{m}$, we have that the inverse of the product exists. Multiplying both sides of (3) by this inverse gives us $a^{\phi(m)} \equiv 1 \pmod{m}$.

□

2 Euler's Totient Function

While it is very nice to have a version of Fermat's Little Theorem for non-prime moduli, it is only of limited use if we don't have a good way of determining the value of $\phi(m)$.[2] In this next section, we derive a formula for $\phi(m)$ based on the prime factorization of m.

2.1 Multiplicative Properties

The first thing that we will need to prove in order to give a formula for $\phi(m)$ is that ϕ is *multiplicative*. In particular, we have the following lemma:

Lemma B2.1. *If m and n are coprime, then $\phi(mn) = \phi(m)\phi(n)$.*

Proof. Consider the function b from $\mathbb{Z}_{mn}$ to $\mathbb{Z}_m \times \mathbb{Z}_n$ given by $b(x) = (x \bmod m, x \bmod n)$. By the Chinese Remainder Theorem from note 6.5, we know that we can uniquely recover the value of x mod mn from its values mod m and mod n. In other words, b is invertible, and hence is a bijection.

Now suppose that $b(x) = (y,z)$. I claim that x is invertible modulo mn if and only if y is invertible mod m and z is invertible mod n. For the "only if" direction, note that if $x^{-1} \pmod{mn}$ exists, $xx^{-1} \equiv 1 \pmod{mn}$, and hence is also 1 mod m and mod n. Thus, x^{-1} mod m is the inverse of y mod m, and x^{-1} mod n is the inverse

[2] This function ϕ is often referred to as Euler's Totient Function

of z mod n. For the if direction, the Chinese Remainder Theorem tells us that there is an $x' \in \mathbb{Z}_{mn}$ such that $x' \equiv y^{-1} \pmod{m}$ and $x' \equiv z^{-1} \pmod{n}$. But then we note that $xx' = 1$ is a solution to the congruences $xx' \equiv 1 \pmod{m}$ and $xx' \equiv 1 \pmod{n}$ — and by the Chinese Remainder Theorem, this solution is unique. Thus, we must have that $xx' \equiv 1 \pmod{mn}$, meaning that x has an inverse mod mn.

Since b is a bijection, it now suffices for us to count how many pairs (y,z) there are such that $y \in \mathbb{Z}_m$ and $z \in \mathbb{Z}_n$ with $\gcd(y,m) = \gcd(z,n) = 1$; each such pair will correspond to exactly one $x \in \mathbb{Z}_{mn}$ such that $\gcd(x,mn) = 1$.[3] But we know that there are $\phi(m)$ choices for y and $\phi(n)$ choices for z. Since these two choices can be made independently of one another, we have a total of $\phi(m)\phi(n)$ choices for the pair (y,z), and hence $\phi(m)\phi(n)$ choices for x. The number of choices for x is by definition $\phi(mn)$, so we indeed have $\phi(mn) = \phi(m)\phi(n)$.

□

2.2 Prime Powers

The previous section tells us that we can split the problem of finding $\phi(m)$ into the problem of finding the value of ϕ on two coprime factors of m. Thus, our strategy for finding $\phi(m)$ will boil down to repeatedly applying this principle until we can't any more. The only point we can't do this at is if m has only one (possibly repeated) prime factor; that is, if m is of the form p^k for some prime p. In this section, we show how to calculate ϕ in this case.

Lemma B2.2. *Let p be a prime and k be a positive integer. Then $\phi(p^k) = (p-1)p^{k-1}$.*

Proof. Consider the set of numbers modulo p^k; for ease of notation later on in the proof, we will use p^k as the "representative" for 0. Thus, we wish to know how many numbers in $\{1,2,...,p^k\}$ are coprime to p^k. It turns out that it is easier to ask how many numbers in this set are *not* coprime to p^k, as these are precisely the multiples of p.

The multiples of p are $p, 2p, 3p, ..., p^k$. Noting that $p^k = (p^{k-1})p$, we have that there are p^{k-1} multiples of p in our set. Hence, the number of non-multiples of p in the set is just the total number of elements in the set minus the number of multiples of p; this works out to $p^k - p^{k-1} = (p-1)p^{k-1}$, as desired.

□

2.3 A General Formula

We can now combine lemmas 2.1 and 2.2 to get a general formula for $\phi(m)$ that works for all m.

Theorem B2.2. *Let $m \geq 2$ be an integer, and let m's prime factorization be $p_1^{n_1} \cdot ... \cdot p_k^{n_k}$. Then we can write $\phi(m) = (p_1 - 1)p_1^{n_1-1} \cdot ... \cdot (p_k - 1)p_k^{n_k-1}$.*

Proof. We first note that $p_k^{n_k}$ is coprime to the rest of m's prime factorization. Hence, by lemma 2.1, we have $\phi(p_1^{n_1} \cdot ... \cdot p_k^{n_k}) = \phi(p_1^{n_1} \cdot ... \cdot p_{k-1}^{n_{k-1}})\phi(p_k^{n_k})$. But then $p_{k-1}^{n_{k-1}}$ is also coprime with everything else in m's factorization, so we can repeat the same trick to pull $\phi(p_{k-1}^{n_{k-1}})$ out. Repeating this for each p_i, we eventually get that $\phi(m) = \phi(p_1^{n_1}) \cdot ... \cdot \phi(p_k^{n_k})$. Applying lemma 2.2 to each term in this product gives us the desired formula for $\phi(m)$.

□

[3] Here, we are using the fact that "x is relatively prime to mn" is equivalent to "x has a multiplicative inverse mod mn".