Number Theory: Totient Function, Residue Classes, Euler and Fermat

Patrick Girardet

October 28, 2013

1 Introduction

In this article we'll be exploring how things like GCD and modular arithmetic interact, giving us powerful results like Euler's Theorem and Fermat's Little Theorem as corollaries. The proofs later on might get a little intimidating with their details, but the point is to formally prove results that you naturally gain intuition for with experience working with mods.

2 Division and Complete Sets of Residue Classes

2.1 Division in Mods

A theme you'll see throughout this handout is that nice things happen in number theory between two numbers if those numbers are relatively prime. We've seen that addition, subtraction, and multiplication all behave very nicely and as we would expect them to without any complications under mods. What about division? More precisely, if we have $ad \equiv bd \pmod{m}$, does this necessarily imply that $a \equiv b \pmod{m}$? Well, no. For a simple counterexample, note that while $3 * 2 \equiv 5 * 2 \pmod{4}$, $3 \not\equiv 5 \pmod{4}$. But wait, $(4, 2) = 2$. That is, the thing we wanted to cancel from both sides was not relatively prime to the modulus. Maybe that has something to do with it? We won't prove this here, but in general, if $(d, m) = 1$, $ad \equiv bd \pmod{m} \Rightarrow a \equiv b \pmod{m}$. More generally, $ad \equiv bd \pmod{m} \Rightarrow a \equiv b \pmod{m/(d, m)}$. To check that this generalization fits our above example, we have that $3 \equiv 5 \pmod{4/(4, 2) = 2}$. We will use these divisibility results later in the handout.

2.2 Complete Sets of Residue Classes

We call the natural numbers $0, 1, ..., n-1$ the **residue classes mod n**. A set of natural numbers S is called a **complete set of residue classes mod n** if it has all of the residue classes mod n when we reduce all of its entries. More formally, $\forall 0 \leq i \leq n-1, \exists k \in S$ such that $k \equiv i \pmod{n}$. Define the following operations on arbitrary sets of numbers: given some numbers a, b, $aS + b$ is the set when we take every entry in S and multiply it by a and add b. Formally, $aS + b = \{ak + b : k \in S\}$. Let's now prove some basic results about the properties of complete sets of residue classes.

Proposition 1: If S is a complete set of residue classes mod n, then aS is also a complete set of residue classes mod n if and only if $(a, n) = 1$.

We first show that aS is a complete set of residue classes if $(a, n) = 1$. Because this set has exactly n elements (since we've reduced everything mod n and we don't count repeated elements in sets), it suffices to show that elements in the set are not congruent to each other modulo n. Assume to the contrary that $ai \equiv aj \pmod{n}$ for some $1 \leq i < j \leq n$. Because $(a, n) = 1$, $i \equiv j \pmod{n}$ by division, which is impossible since $|i - j| < n$. Hence our assumption that some elements were congruent was wrong and aS is a complete set of residue classes.

On the other hand (we now prove the only if direction), if $g = (a, n) > 1$, then $a = a_1 g, n = n_1 g$ where n_1 is some positive integer less than n. By substituting in these definitions, we have $an_1 \equiv a_1 n_1 g \equiv a_1 n \equiv an \equiv 0 \pmod{n}$, which means that we don't have a complete set of residue classes since we have $an_1 \equiv an \pmod{n}$ for some n_1 smaller than n.

We can prove a similar result (though we don't do so here):

Proposition 2: Let n be a positive integer. Let a be an integer relatively prime to n, and let b be an integer. If S is a complete set of residue classes modulo n, then the set $aS + b$ is also a complete set of residue classes modulo n.

Now that we've prove some essential facts about complete sets of residue classes, let's take a slight detour.

3 Euler's Totient Function

Before we define this function, recall that we call two integers a, b **relatively prime** if their GCD is 1, that is, $(a, b) = 1$ using the parentheses notation for GCD.
We define the Euler totient function $\phi(n)$ for positive integers n as the number of positive integers less than n and relatively prime to n. We now discuss some critical properties of this function.
First off, note that $\phi(p) = p - 1$ for prime numbers p by the definition of prime numbers. Similarly, $\phi(p^k) = p^{k-1}(p-1) = p^k(1 - \frac{1}{p})$ for positive integers k and primes p, as every number less than p^k is relatively prime to it except the multiples of p.
A less trivial property of $\phi(n)$ is that it is **multiplicative**, that is, if $(a, b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$. (If we removed the condition that a and b are relatively prime, we would have a **totally multiplicative** function, which is in fact proper mathematical terminology and not teen-speak infiltrating the lexicon of academia.)
Proof: Arrange the integers $1, 2, ..., ab$ into an $a \times b$ array as follows:

$$\begin{array}{cccc} 1 & 2 & & ...a \\ a+1 & a+2 & & ...2a \\ . & . & . & \\ . & . & . & \\ . & . & . & \\ a(b-1)+1 & a(b-1)+2 & & ...ab \end{array}$$

Clearly, there are $\phi(ab)$ numbers in the above table that are relatively prime to ab. On the other hand, there are $\phi(a)$ columns containing those elements in the table relatively prime to a. Each of those columns is a complete set of residue classes modulo b, by Proposition 2. Hence there are exactly $\phi(b)$ elements in each of those columns that are relatively prime to b. Therefore, there are $\phi(a)\phi(b)$ numbers in the table that are relatively prime to ab. Hence, $\phi(ab) = \phi(a)\phi(b)$ for relatively prime integers ab.
This lets us compute $\phi(n)$ for arbitrary n given the prime factorization of n. Let n have the general prime factorization $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$. By using that $\phi(n)$ is multiplicative and that $(p_i, p_j) = 1$ if $i \neq j$, $\phi(n) = \phi(p_1^{e_1} p_2^{e_2} ... p_k^{e_k}) = \phi(p_1^{e_1})\phi(p_2^{e_2})...\phi(p_k^{e_k})$. However, we know how to evaluate these individual phi functions! This evaluates to $p_1^{e_1}(1 - \frac{1}{p_1})p_2^{e_2}(1 - \frac{1}{p_2})...p_k^{e_k}(1 - \frac{1}{p_k})$. We notice that all of the $p_i^{e_i}$ from the original prime factorization pop up in this product. Thus, we can pull them all out to the side to just get n, giving us that $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_k})$. This should sort of make sense: the $(1 - \frac{1}{p_i})$ terms serve

to "filter out" the multiples of the primes, which occur with a frequency of $(1 - \frac{1}{p_i})$. This isn't a rigorous proof, but there is a proof of this formula for the totient function using PIE which makes this idea clearer. Now let's put this interesting function to work.

4 Euler's and Fermat's Little Theorems

Before proving these results which we've been working up to through this handout, let's take a brief definition detour.

We call a set of integers S a **complete reduced set of residues mod n** if it has all the residues relatively prime to n. Formally, S is a complete reduced set of residues mod n if $\forall i$ such that $(i, n) = 1$, $\exists k \in S$ such that $k \equiv i \pmod{n}$. Clearly, a complete reduced set of residues mod n has $\phi(n)$ elements. A result which we won't prove here but whose proof is similar to the proof for the same result on standard complete sets of residues is the following:

Proposition 3: If S is a complete reduced set of residues modulo n, and $(a, n) = 1$, then aS is a complete reduced set of residues modulo n.

We can now get to proving Euler's theorem and Fermat's little theorem as a corollary.

Euler's theorem: If $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

That's a pretty ridiculous looking expression. To the power of the totient function? What? But 'tis true.

Proof: Consider some complete reduced set of residues modulo n $S = \{b_1, b_2, ..., b_{\phi(n)}\}$. We have from the conditions of the theorem that a and n are relatively prime. Thus, aS is a complete reduced set of residues modulo n by Proposition 3. Since S and aS are both complete reduced sets of residues modulo n, the product of all their elements is the same modulo n. That is, taking the product of all the elements in aS on the left and the elements in S on the right, we have $(ab_1)(ab_2)...(ab_{\phi(n)}) \equiv b_1 b_2 ... b_{\phi(n)} \pmod{n}$. Since the a_i are relatively prime to n, we can divide them out by our divisibility criteria. Thus, we are left with the product of all the as on the left and simply 1 on the right, and since there was one a for each of the $\phi(n)$ b_i, we have our desired $a^{\phi(n)} \equiv 1 \pmod{n}$.

If we plug in p prime into this formula, we get **Fermat's Little Theorem**: $a^{p-1} \equiv 1 \pmod{p}$.

These formulae have a number of applications: not only do they serve as a bedrock for further number theory study into things like orders and primitive roots, but they can often be used in math competition problems where you might need to evaluate some number exponentiated mod something else. An olympiad number theory article with competition problems that presupposes knowledge of these theorems can be found here: `http://www.artofproblemsolving.com/Forum/viewtopic.php?f=721&t=547759&hilit=olympiad+number+theory`