CLASS 17, GIVEN ON 10/29/2010, FOR MATH 25

1. A generalization of Fermat's Little Theorem

Let us change gears from trying to solve $f(x) \equiv 0 \mod p^e$ and go back to Fermat's Little Theorem. It says that if p is prime, and $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$. Equivalently, we can drop the restriction on a, and then $a^p \equiv a \mod p$.

What if the modulus is not prime? Is there some sort of statement like this? A bit of thought will show that $a^{n-1} \equiv 1 \mod n$ can be false for lots of values of a if n is composite; for instance, if $n = 4$, then $a^3 \equiv 1 \mod 4$ if and only if $a \equiv 1 \mod 4$. So this is not so promising.

The correct statement is the following theorem:

Theorem 1 (Fermat-Euler Theorem, Theorem 5.3)**.** *Let n be any positive integer, and let a be an integer such that* $\gcd(a, n) = 1$. *Then*

$$a^{\phi(n)} \equiv 1 \mod n.$$

(Recall that $\phi(n)$ is the Euler phi function, which tells us the number of positive integers less than or equal to n which are relatively prime to n.)

Before proving this, let's look at a few examples.

- This is called the Fermat-Euler theorem not because Fermat codiscovered it with Euler (Fermat died about 40 years before Euler was born), but because Euler discovered this theorem, which is a generalization of Fermat's Little Theorem. Indeed, if n is prime, then $\phi(n) = n - 1$, and the condition $\gcd(a, n) = 1$ is equivalent to $n \nmid a$.
- Let $n = 12$. Some quick calculation shows that $\phi(12) = 4$. Then $a^4 \equiv 1 \mod 12$ if $a \equiv 1, 5, 7, 11 \mod 12$.

Proof. (Proof of Fermat-Euler theorem) The basic idea behind proving the Fermat-Euler theorem is the same as the proof of Fermat's Little Theorem. Let $r_1, \dots, r_{\phi(n)}$ be a complete set of representatives mod n of congruence classes which are relatively prime to n; for instance, if we require $1 \le r_i \le n$, then we can choose the r_i to be the $\phi(n)$ positive numbers $\le n$ which are relatively prime to n.

Let a be any integer with $\gcd(a, n) = 1$, as specified in the theorem. We claim that $ar_1, \dots, ar_{\phi(n)}$ is still a complete set of representatives mod n of congruence classes relatively prime to n. Indeed, since $\gcd(r_i, n) = \gcd(a, n) = 1$, it is true that $\gcd(ar_i, n) = 1$ for all i. So it only remains to check that all the ar_i are inequivalent to each other; this is clear since $ar_i \equiv ar_j \mod n$ implies $a(r_i - r_j) \equiv 0 \mod n$. Since $\gcd(a, n) = 1$, we can cancel out a from both sides of the congruence, so this implies $r_i \equiv r_j \mod n$. And the original definition of the r_i forces $r_i = r_j$, as desired.

So mod n, the set $ar_1, \dots, ar_{\phi(n)}$ is a rearrangement of the set $r_1, \dots, r_{\phi(n)}$. Multiply each of these lists together; we get

$$r_1 \dots r_{\phi(n)} \equiv (ar_1) \dots (ar_{\phi(n)}) = a^{\phi(n)}(r_1 \dots r_{\phi(n)}) \mod n.$$

On the other hand, since all the r_i are relatively prime to n, we can cancel them all out from both sides of the congruence. We are left with

$$a^{\phi(n)} \equiv 1 \mod n,$$

which was what we wanted to prove. $\square$

Example. As an illustration of the idea behind the proof, suppose $n = 8$. Then a complete set of representatives of congruence classes mod 8 relatively prime to 8 is given by $1, 3, 5, 7$. Let a be any number relatively prime to 8; say, $a = 3$. Then $a, 3a, 5a, 7a = 3, 9, 15, 21$ is still a complete set of representatives of congruence classes mod 8 relatively prime to 8, since $3, 9, 15, 21 \equiv 3, 1, 7, 5 \mod 8$. In particular, $(1)(3)(5)(7) \equiv (3)(9)(15)(21) = 3^4(1)(3)(5)(7) \mod 8$, which implies that $3^4 \equiv 1 \mod 8$.

2. Calculating $\phi(n)$

In order to use the Fermat-Euler theorem, we might want to calculate $\phi(n)$. And in any case, it is an interesting question to actually determine a formula for $\phi(n)$.

We already know what happens if n is a prime p. Then it is clear that $\phi(p) = p - 1$. We can extend this to prime powers fairly easily:

Lemma 1 (Lemma 5.4)**.** *For p prime, $e \geq 1$, $\phi(p^e) = p^e(1 - 1/p) = p^e - p^{e-1}$.*

Proof. It is clear that $\gcd(a, p^e) = 1$ if and only if $p \nmid a$. To calculate $\phi(p^e)$, then, we want to count the number of integers in the list $1, 2, \ldots, p^e$ which are not divisible by p. But this is easy to do; the number which are divisible by p is clearly p^{e-1} (in any case, this was a homework problem). So $\phi(p^e) = p^e - p^{e-1}$, as desired. $\square$

Right now, we can calculate $\phi(n)$ when n is a prime, or more generally, a prime power. We know that every integer n is a (unique) product of prime powers. So if we can find a way to express $\phi(n)$ in terms of $\phi(p^e)$, for the various p^e appearing in the prime factorization of n, we will have a formula for $\phi(n)$. The following lemma will help us:

Lemma 2. *Let m, n be relatively prime positive integers. Let $a_1, \ldots, a_m$ be a complete set of residues mod m, and let $b_1, \ldots, b_n$ be a complete set of residues mod n. Then $na_i + mb_j$, where $1 \leq i \leq m, 1 \leq j \leq n$, form a complete set of residues mod mn.*

Proof. Clearly there are mn elements in the list $na_i + mb_j$ as i, j vary. Therefore, to show that this is a complete set of representatives, it suffices to show that any two different choices for the ordered pair (i, j) give distinct classes mod mn.

Suppose that $na_i + mb_j \equiv na_{i'} + mb_{j'} \mod mn$. Moving everything to the left side, this is the same as

$$n(a_i - a_{i'}) + m(b_j - b_{j'}) \equiv 0 \mod mn.$$

Because m, n are relatively prime, this is true if and only if the two following congruences are simultaneously true:

$$n(a_i - a_{i'}) + m(b_j - b_{j'}) \equiv 0 \mod m, n(a_i - a_{i'}) + m(b_j - b_{j'}) \equiv 0 \mod n.$$

In the first congruence, notice that m always divides the second term, regardless of what j, j' are. So the first congruence is equivalent to $n(a_i - a_{i'}) \equiv 0 \mod m$. We again use the fact that m, n are relatively prime to divide both sides of the congruence by n, to reach the equivalent congruence $a_i - a_{i'} \equiv 0 \mod m$. In a similar way, we find the second congruence in our list above is equivalent to $b_j - b_{j'} \equiv 0 \mod n$.

Now we use the fact that the a_i, b_j were a complete set of representatives mod m, n respectively. The only way these two congruences can be true is if $a_i = a_{i'}, b_j = b_{j'}$, which is what we wanted to prove. $\square$

Example. Let $m = 2, n = 3$, and let $a_1, a_2 = 0, 1$, $b_1, b_2, b_3 = 0, 1, 2$. Then the previous lemma says that $3a + 2b$, as a, b vary across $a = 0, 1, b = 0, 1, 2$, give a complete set of representatives mod 6. Indeed, the values are $0, 2, 4, 3, 5, 7 \equiv 0, 2, 4, 3, 5, 1 \mod 6$.

Using this, we can now prove the following theorem:

Theorem 2 (Theorem 5.6)**.** *If m, n are relatively prime, then $\phi(mn) = \phi(m)\phi(n)$.*

Proof. Let $a_i, 1 \le i \le m$ be a complete set of representatives mod m, and similarly let $b_j, 1 \le j \le n$ be a complete set mod n. The previous lemma tells us $na + mb$ is a complete set mod mn, as a, b range across a_i, b_j respectively.

If necessary, relabel the a_i, b_j to ensure that $a_1, \dots, a_{\phi(m)}$ form a complete set of representatives mod m which are relatively prime to m, and similarly for $b_1, \dots, b_{\phi(n)}$. We claim that $na + mb$ is relatively prime to mn if and only if a is one of the $a_1, \dots, a_{\phi(m)}$, and b is one of the $b_1, \dots, b_{\phi(n)}$.

Indeed, $\gcd(na+mb, mn) = 1$ if and only if $\gcd(na+mb, m) = 1$ and $\gcd(na+mb, n) = 1$. Since mb is a multiple of m, regardless of the value of b, $\gcd(na + mb, m) = 1$ if and only if $\gcd(na, m) = 1$. Since $\gcd(n, m) = 1$, this is true if and only if $\gcd(a, m) = 1$, which means that a is one of the $a_i, 1 \le i \le \phi(m)$. Similarly, $\gcd(na + mb, n) = 1$ if and only if b is one of the $b_j, 1 \le j \le \phi(n)$.

Notice that the number of elements in $na + mb$ which are relatively prime to mn is the same as $\phi(mn)$. Indeed, since $na + mb$ gives a complete set of representatives mod mn, the remainders of these numbers are some re-ordering of $0, 1, 2, \dots, mn - 1$, and the number of elements in this list which are relatively prime to mn is just $\phi(mn)$. Since the property of a number k being relatively prime to mn is only dependent on $k \mod mn$, a number $na + mb$ is relatively prime to mn if and only if its remainder after division by nm is also relatively prime to mn.

We have shown that $na + mb$ is relatively prime to mn if and only if a, b are relatively prime to m, n respectively. There are $\phi(m)$ choices for such a and $\phi(n)$ choices for such n; therefore there are $\phi(m)\phi(n)$ $na + mb$ which are relatively prime to mn, and we already knew that each of these $na + mb$ were distinct mod mn. Therefore $\phi(m)\phi(n) = \phi(mn)$, as desired.

□

The book uses a slightly different method to prove this theorem. Instead of looking at $na + mb$, the book considers $na + b$, where $0 \le a < m, 1 \le b \le m$. As a, b vary in these intervals, $na + b$ lists all the numbers $1, 2, \dots, nm$ exactly once. The book then shows that $\gcd(na + b, mn) = 1$ if and only if $\gcd(a, m) = 1$ and $\gcd(b, n) = 1$, and then counting the number of possible choices for a, b yields the theorem. Yet another idea for proving this theorem is to use the Chinese Remainder Theorem (see HW assignment 6).

This theorem provides all the information we need to compute $\phi(n)$, assuming that we can factor n. If $n = p_1^{e_1} \dots p_k^{e_k}$, then

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

In general, a function $f : \mathbb{N} \to \mathbb{N}$, or more generally $f : \mathbb{N} \to \mathbb{R}$ or $\mathbb{C}$ is called *multiplicative* if $f(1) = 1$, and $f(mn) = f(m)f(n)$ whenever m, n are relatively prime. So the previous theorem tells us that ϕ is a multiplicative function. Notice that every multiplicative function is completely determined by its values on prime powers. In number theory, there are many different multiplicative functions which are important; we will come across a few more later on in this class.

Examples.

- Calculate $\phi(100)$. Instead of listing all the numbers from 1 to 100 and then determining which are relatively prime to 100 (a painful thing to do), we can use the above formula. The first step is to factor $100 = 2^2 \cdot 5^2$. Then $\phi(100) = \phi(2^2)\phi(5^2) = (4-2)(25-5) = 40$.
- A listing of the first few values of ϕ gives $1, 1, 2, 2, 4, 2, 6, 4, \ldots$. We will show that $\phi(n)$ is odd only for $n = 1, 2$. Indeed, first notice that if p is an odd prime, then $\phi(p^e)$ is even for any $e \geq 1$, since $\phi(p^e) = p^e - p^{e-1}$ is a difference of two odd numbers. So if n has an odd prime factor p, then $\phi(n)$ will be even, since $\phi(p^e)$ divides $\phi(n)$ and $\phi(p^e)$ is even.

  So suppose n has no odd prime factors; ie, is a power of 2. Then $\phi(2^e) = 2^e - 2^{e-1} = 2^{e-1}$. Clearly this is odd only when $e = 1$ (this formula is not applicable when $e = 0$). So $\phi(n)$ is only odd for $n = 1, 2$.
- We say that $a \mod n$ is a *unit* mod n if it has a multiplicative inverse; that is, there exists a number $b \mod n$ such that $ab \equiv 1 \mod n$. For instance, when $n = 4$, $1, 3 \mod 4$ are units, while $0, 2 \mod 4$ are not. Recall that we saw that $a \mod n$ has a multiplicative inverse if and only if $\gcd(a, n) = 1$. Therefore, the number of units mod n is equal to $\phi(n)$.

We conclude with a proposition whose importance is not apparent right now, but is interesting and has a neat method of proof. In about a week we will see how this proposition can be applied to prove other theorems.

Proposition 1. *Let n be a positive integer. Then*

$$\sum_{d|n} \phi(d) = n,$$

where the summation runs over all positive divisors of n, including 1 and n.

Proof. We will group up all the numbers from $1, 2, \ldots, n$ into various sets depending on their gcd with n. Let S_d be the subset of $1, 2, \ldots, n$ which consists of all the integers whose gcd with n is exactly equal to n/d. In set theoretic notation, $S_d = \{a \,|\, 1 \leq a \leq n, \gcd(a, n) = n/d\}$.

The first claim is that the various sets S_d, as d ranges over divisors of n, partition $1, 2, \ldots, n$. First, notice every $a, 1 \leq a \leq n$, is a member of some S_d with $d \mid n$, since $\gcd(a, n) \mid n$. Furthermore, all these sets are disjoint, since $\gcd(a, n)$ is a fixed number, so that a can only belong to $S_{\gcd(a,n)}$.

This means that the sum of the sizes of S_d is equal to the size of the set $\{1, 2, \ldots, n\}$, which clearly is n. Therefore, to prove the proposition it is enough to show that each S_d has size $\phi(d)$.

A number a is an element of S_d if and only if $1 \leq a \leq n$ and $\gcd(a, n) = n/d$. This in turn is equivalent to there being an a' such that $a = (n/d)a', 1 \leq a' \leq d$, and $\gcd(a', d) = 1$. The first two conditions are fairly clear; for the last, recall that if d is a common divisor of a, b, then $\gcd(a/d, b/d) = \gcd(a, b)/d$. How many choices of a' are there? Exactly $\phi(d)$. Therefore, S_d has size $\phi(d)$ as claimed. $\square$

Example. As an illustration of the idea of the proof, let $n = 12$. Then S_{12} consists of the numbers from 1 to 12 which have gcd $12/12 = 1$ with n; we quickly see that $S_{12} = \{1, 5, 7, 11\}$. Similarly, S_6 consists of those numbers from 1 to 12 which have gcd $12/6 = 2$ with $n = 12$. One sees that $S_6 = \{2, 10\}$. For $d = 4, 3, 2, 1$, one checks that $S_4 = \{3, 9\}, S_3 = \{4, 8\}, S_2 = \{6\}, S_1 = \{12\}$. You can quickly check that every number from 1 to 12 lies in exactly one of these sets, and that the size of S_d is $\phi(d)$.