Quick Summary of Last Time

Proved Fermat's Theorem: if gcd(a,p) = 1 and p is prime, then $a^{p-1} = 1 \bmod p$

Started talking about trying to get an equivalent formula for non-prime numbers.

Euler Phi Function: $\phi(n)$ = the number of integers, x, in the set {1, 2, 3, …, n-1} such that gcd(x, n) = 1.

$\phi(p) = p - 1$, p is prime

$\phi(pq) = (p-1)(q-1)$, p and q are distinct primes.

Today's Goal

1) Come up with a formula to calculate $\phi(n)$, for all positive integers n > 1.
2) Prove Euler's Theorem: if gcd(a,n) = 1, then $a^{\phi(n)} = 1 \bmod p$

Phi Calculation

$\phi(p^k) =$?

{1, 2, 3, …, p, p+1, 2p+1, …, $p^k - 1$, p^k} is my set. (Note: Added the last element knowing we will cross it off.

We want to cross out everything that shares a common factor with p^k?

Example 2^4? {1,2,3,4,…,15,16} Every other number shares a common factor with 2. So 16/2.

More generally, one out of every p values will get crossed off. Those values are:

p, 2p, 3p, 4p, … $p^{k-1}(p)$

How many values are on this list? p^{k-1}

$$\phi(p^k) = p^k - p^{k-1}$$

How on earth are we going to get a formula for every number???

One thing to realize is that there are lots of different molds of prime factorizations, so I can't possible, go through all of them.

BUT, if I can prove more general property about the phi function in general, then maybe I can use that property and apply it to all number!

It turns out that the phi function is multiplicative…

if gcd(m,n) = 1, then $\phi(mn) = \phi(m)\phi(n)$.

then $\phi(2^3 3^2 7^1) = \phi(2^3 3^2)\phi(7) = \phi(2^3)\phi(3^2)\phi(7) = (2^3 - 2^2)(3^2 - 3)(7 - 1) = 144$

Let's try to prove it!

if gcd(m,n) = 1, then $\phi(mn) = \phi(m)\phi(n)$.

List out all the numbers in our set:

1	2	3	4	…	m
m+1	m+2	m+3	m+4	…	2m
2m+1 …					
3m+1 …					
…					
(n-1)m+1					nm

Very quickly, we can cross off each number in the last row. But since m is NOT prime, there may be other rows that get crossed off. In fact, for each row that has a number that shares a common factor with m, the top value in that row gets crossed off, and all the values in that row get crossed off because if m shares a common factor with some integer k, then m shares a common factor with k+m or k+2m.

So far, we've crossed off $n \times \big(m - \phi(m)\big)$, which means that there are $n \times \big(\phi(m)\big)$ that are NOT crossed off.

Consider any column that is NOT crossed off, so for example:

1, m+1, 2m+1, …, (n-1)m+1

In general, one of these columns will look like

k, m+k, 2m+k, …, (n-1)m+k, where 1 <= k < n.

Now, we need to cross off values that share a common factor with n. Instead of doing all of these, columns, let's just do one arbitrary column.

We know gcd(m, k) = 1. But some of these values may share a common factor with n.

We want to count how many share a common factor with n and cross those off.

We could count how many do NOT share a common factor with n.

Consider the values in this set mod n

k mod n

M+k mod n

2m + k mod n

3m + k mod n…

(n-1)m + k mod n

Want to see how many different mod values we get mod n.

There are n values listed total.

We will prove that each unique mod value appears on this list.

Formally, we will prove that no two values on the list are equivalent mod n via proof by contradiction.

Assume to the contrary that two values on the list above are equivalent mod n:

im + k = jm+k (mod n), where 0 <= i < j < n

im = jm (mod n)

im – jm = 0 (mod n)

m(i-j) = 0 (mod n)

Number theory result: if gcd(a,b) = 1, and b | ac, then b | c.

n | (m(i-j)) AND gcd(m,n) = 1, therefore n | (i-j).

But… 0 < |i-j| < n, but this contradicts our finding that n | (i-j). So we must conclude that our initial assumption was wrong, so there is no pair values on the list that are equivalent mod n.

So…each column has every unique value mod n, and it follows that precisely $\phi(n)$ values in each of these columns share no common factor with m, and there were $\phi(m)$ columns to consider, so that all the values we didn't cross off equals $\phi(n) \times \phi(m)$.

Let's try out n = 4, m = 15

1	~~2~~	3	~~4~~	5	6	7	~~8~~	9	10	11	12	13	~~14~~	15
~~16~~	17	18	19	20	21	~~22~~	23	24	25	~~26~~	27	~~28~~	29	30
31	~~32~~	33	~~34~~	35	36	37	~~38~~	39	40	41	42	43	~~44~~	45
~~46~~	47	48	49	50	51	~~52~~	53	54	55	~~56~~	57	~~58~~	59	60

7 columns crossed off, 8 are still alive. We want to cancel out even values.

When we are done, the values that are left are in $\phi(15) = 8$ columns, and for each column there are a total of $\phi(4) = 2$ values that remain after crossing out the other values.

Euler's Theorem Proof

Start with a set of values from to 1 to n, where each value does NOT share a common factor with n. Thus, the set has $\phi(n)$ values in it.

Example: n = 15, S = {1,2,4,7,8,11,13,14}

Pick any a such that gcd(a, n) = 1. Let a = 7

T = {7, 14, 28, 49, 56, 77, 91, 98} (all values in S multiplied by a)

S = { a_1, $a_{2, \ldots,} a_{\phi(n)}$}

T = { aa_1, $aa_{2, \ldots,} aa_{\phi(n)}$}

We want to prove that the values in the set T are all equivalent to the values in the set S mod n.