Nicole Robles

CYEN 489 – 001

Proofs Homework 2 – Euler Phi Function

Conjecture 1:

$\varphi(p) = p - 1$, when p is prime

Proof 1:

Since p in the conjecture is a prime number, the only factors that can divide it are 1 and itself (p). For every prime number p, the numbers relatively prime to it would be every integer from 1 to one less than p. Since this number is $p - 1$, this proves the conjecture that $\varphi(p) = p - 1$.

■

Conjecture 2:

$\varphi(m * n) = \varphi(m) * \varphi(n)$, when p is prime and $\gcd(m, n) = 1$

Proof 2:

The set of integers {1, 2, 3, ..., m*n} is shown below.

1	m+1	2m+1	...	(n-1)*m+1
2	m+2	2m+2	...	(n-1)*m+2
3	m+3	2m+3	...	(n-1)*m+3
...	...	...	...	...
r	m+r	2m+r	...	(n-1)*m+r
...	...	...	...	...
m	2m	3m	...	m*n

There exists a $d = \gcd(m, r)$ such that d|m and d|r. Every element in the r^{th} row is not relatively prime to $m * n$, meaning any element of this row is of the form $k * m + r$ where $k \in \{1, \dots, n - 1\}$ and d|$(k * m + r)$ because d|m and d|r. This means that the amount of relatively prime rows left is $\varphi(m)$.

If $\gcd(m, r) = 1$, then $i * m + r \equiv j * m + r \ (mod\ n), i \neq j$ is a complete system of residues modulo n. In other words, the numbers in each row that are relatively prime to n can be denoted as $\varphi(n)$ through Proof 1. Multiplying the relatively prime rows by the relatively prime candidates in each row, we get $\varphi(m) * \varphi(n)$, which matches Conjecture 2 stated above, thus completing the proof.

■

Conjecture 3:

$$\varphi(p^m) = (p-1)p^{m-1} = \varphi(p) * p^{m-1}, \text{ when p is prime}$$

Proof 3:

The set of integers {1, 2, 3, ..., p^m} is shown below.

1	p+1	2p+1	...	$p^{m-1}+1$
2	p+2	2p+2	...	$p^{m-1}+2$
3	p+3	2p+3	...	$p^{m-1}+3$
...	...	...	...	...
p	2p	3p	...	p^m

p is assumed to be a prime number, so the only values that can divide it are multiples of itself, from p to p^m. The only row that would be divisible by p is the last row in the table, since it has the multiples of p. Therefore, the number of rows that would be relatively prime to p would be $p-1$. Since there are p^{m-1} columns in the table, we can multiply the number of rows relatively prime to p by the number of columns in order to get $(p-1) * p^{m-1}$. Based on the equation proven in Proof 1 where $\varphi(p) = p - 1$, the final equation can be written as $\varphi(p) * p^{m-1}$, thus completing the proof.

■