Euler's Phi function for Powers of Primes

Elaine Chetcuti

The Phi function $\phi(n)$ is defined as the number of positive integers less than n which have no factor in common with n.

Knowing that a residue group is a set of positive integers less than n and relatively prime to n; the phi function, $\phi(n)$, can be defined as the number of elements in the residue group.

$\phi(n)$ = no. of natural numbers $< n$: (a, n) =1

Consider $\phi(4)$:

There are 2 positive integers less than 4 which have no common factor with 4 namely (1 and 3). Hence

- $\phi(4) = 2$

Consider $\phi(7)$:

There are no positive integers less than 7 which have a common factor with 7 since 7 is a prime number.

Therefore we can say that for any prime number p, $\phi(p) = p$-1

Our attempt is to find $\phi(p^k)$

Let us consider $\o(p^2)$

Consider first $\o(5^2)$

Listing all positive integers less than 25, we obtain

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

1 2... pp+1...... $2p2p$+1.............$3p3p$+1.............$4p$

21 22 23 24 25

$4p$+1.............$5p$ (where $5p$ is p^2in this case)

Therefore, to find $\o(p^2)$, first list all positive integers less than p^2

1 2 3..... p, p+1.....$2p$,$2p$+1...$3p$,$3p$+1....p^2

This makes us realize that $p, 2p, 3p, 4p,\ldots p^2$are the only integers which are not coprime with p^2.

Therefore $\o(p^2) = p^2 - p$

Let us now consider $\o(p^3)$

The positive integers from 1 to p^3 can be divided into p sets:

1	to	p^2		($p^2 - p$ coprimes)
p^2+ 1	to	$2p^2$		($p^2 - p$ coprimes)
$2p^2$+ 1	to	$3p^2$		($p^2 - p$ coprimes)
......				
......				
(p-2)p^2+ 1	to	(p-1)p^2		($p^2 - p$ coprimes)
(p-1)p^2+ 1	to	p^3		($p^2 - p$ coprimes)

Each set has $p^2 - p$ coprimes and there are p sets.

$\Rightarrow$ total number of coprimes from 1 to $p^3 = p(p^2 - p)$

$\Rightarrow \varnothing(p^3) = p(p^2 - p)$

$= p^2(p - 1)$

From this we claim that $\varnothing(p^n) = p^{n-1}(p - 1)$

Let us prove this by the Principle of Induction

RTP: $\varnothing(p^n) = p^{n-1}(p - 1)$

Proof

Let $n = 1$

LHS: $\varnothing(p^1) = p-1$ (as discussed earlier)

RHS: $p^{1-1}(p - 1) = p^{1-1}(p - 1) = p^0(p - 1) = (p - 1)$

$\therefore$ true for $n = 1$

Assume it is also true for $n = k$

i.e. $\varnothing(p^k) = p^{k-1}(p - 1)$

We need to prove it is true for $n = k + 1$

i.e. RTP $\varnothing(p^{k+1}) = p^k\ (p - 1)$

The positive integers from 1 to p^{k+1} can be divided into p groups as in the case of 1 to p^3 earlier on

1	to	p^k		($p^{k-1}(p-1)$ coprimes)
$p^k + 1$	to	$2p^k$		($p^{k-1}(p-1)$ coprimes)
$2p^k + 1$	to	$3p^k$		($p^{k-1}(p-1)$ coprimes)
......				
......				
$(p\text{-}2)p^k + 1$	to	$(p\text{-}1)p^k$		($p^{k-1}(p-1)$ coprimes)
$(p\text{-}1)p^k + 1$	to	p^{k+1}		($p^{k-1}(p-1)$ coprimes)

Each set has $p^{k-1}(p-1)$ coprimes and there are p sets.

$\Rightarrow$ total number of coprimes from 1 to $p^{k+1} = p(p^{k-1}(p-1))$

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

$= p^k(p-1)$

As $\phi(p^n) = p^{n-1}(p-1)$ holds for $n = 1$ and whenever it is true for $n = k$, it is also true for $n = k+1$, by the Principle of Induction, the theorem is true for all natural numbers n.