MATH 335 lecture 5

Chris Camano: ccamano@sfsu.edu

September 6, 2022

Euler's ϕ function: The euler's phi function can be defined in the following way.

Take any positive integer. Then $\phi(n) = |\{a \in \mathbb{Z} : q \leq a \leq n, gcd(a,n) = 1\}$ Phi of n counts the number of integers between one and n that are relatively prime to n.

if p is prime then$\phi(p) = p - 1$

if p is a prime number and k is a postive integer then:

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

Proof.

$$\begin{aligned}
&\phi(p^k) = |\{a \in \mathbb{Z}q \leq a \leq p^k, gcd(a,p^k) = 1\}| \\
&p^k - |b \in \mathbb{Z} : 1 \leq b \leq p^k, gcd(b,p^k) \neq 1\}| \\
&p^k - |b \in \mathbb{Z} : 1 \leq b \leq p^k, gcd(b,p^k) = kp, k \in \mathbb{Z}\}| \\
&p^k - |\{p, 2p, 3p, ..., p^{k-1}p\}| \\
&p - p^{k-1} \\
&p^{k-1}(p-1)
\end{aligned}$$

□

If the gcd of a number and a prime power is not equal to one then the gcd must be a multiple of 1.

If $m,n \in \mathbb{Z}^+, gcd(m,n) = 1$ then :

$$\phi(mn) = \phi(m)\phi(n)$$

$$\phi(n) = \prod_{i=1}^{k} \phi(p_i^{\alpha_i}) = \prod_{i=0}^{k} p_i^{\alpha_i - 1}(p_i - 1)$$

$$\phi(nm) = \prod_{i=1}^{k} \phi(p_i^{\alpha_i}) \prod_{i=1}^{k} \phi(p_i^{\beta_i}) = \prod_{i=1}^{k} q_i^{\beta_i - 1}(q_i - 1)p_i^{\alpha_i - 1}(p_i - 1) =$$

Proof. If t is a postive integer and $\prod^k p_i$ are the prime divisiors of t then :

$$\phi(t) = \prod_{i=1}^{k} \phi(p_i^{\alpha_i}) = t - |\{1 \leq a \leq t : gcd(a,t) \neq 1\}|$$

$$\phi(t) = \prod_{i=1}^{k} \phi(p_i^{\alpha_i}) = t - |\{1 \leq a \leq t : \exists p_i : p_i|a|$$

where p_i is one of t's prime factors: Since gcd =1 then:

$$\{\prod_{i=1}^{k} \phi(p_i^{\alpha_i})\} \cap \{\prod_{i=1}^{k} \phi(q_i^{\beta})\} = \emptyset$$

$$\phi(mn) = mn - |\{1 \leq a \leq mn : p_i|a \vee q_j|a\}|$$

This is equivilant to :

$mn - |\{1 \leq b \leq m :$ b is divisble by at least one prime factorof n $|n - |\{1 \leq c \leq n :$ c is dibisble by at least one prime factor of

□