# MATH 314 Spring 2018 - Class Notes

2/22/2018

Scribe: Sultan Alneyadi

**Summary:** Today we covered Euler's Phi function, Euler's theorem and 3 pass-protocol.

## Euler's Phi function(totient function):

**Definition:**

$\varphi$ - Greek letter Phi($\phi$)
$\varphi$(n) = number of residues mod n that are coprime to n
$\varphi(26) = 12$

Chines remainder theorm tells us that for every a and b

$$x \equiv a \pmod{p}$$
$$x \equiv b \pmod{q}$$

a can be anything from 1 to p-1, (p-1) possiblities for a
b can be anything from 1 to q-1, (q-1) possiblities for b

let p be prime
$\varphi$(p) = p-1
suppose q is also prime and $p \neq q$
$\varphi$(pq)
$\varphi(pq) = (p-1)(q-1) = pq(1-\frac{1}{p})(1-\frac{1}{q})$
$\varphi(26) = \varphi(13*2) = (12)(1) = 12$

$\prod \leftarrow$ Multiplication version of $\sum$ for addition

$\varphi(n) = n\prod(1-\frac{1}{p})$
$\varphi(100) = 100\prod(1-\frac{1}{p}) \qquad p \in 2,5$
$= 100(1-\frac{1}{2})(1-\frac{1}{5})$
$= 100(\frac{1}{2})(\frac{4}{5})$
$= 40$

**Euler's Theorem:**

if a and b are coprime then
$a^{\varphi(n)} \equiv 1 \pmod{n}$
if n=p is prime then
$\varphi(p) = p-1$
then Euler's theorem says
$a^{\varphi(p)} = a^{p-1} \equiv 1 \pmod{p} \leftarrow$ Format's little theorem

example:

n=6, let a=5, $a^{\varphi(n)}$

$$\varphi(6) = 6(1-\tfrac{1}{2})(1-\tfrac{1}{3})$$
$$= 6(\tfrac{1}{2})(\tfrac{2}{3})$$
$$= 2$$
$$5^{\varphi(6)} \equiv 5^2 \equiv 1 \pmod{6}$$

General principle for exponents in modular arithmetic: if you are doing arithmetic (mod n) them all that matters in the exponent is the value mod $\varphi(n)$

compute $5^23 \pmod{6}$
since $23 \equiv 1 \pmod{\varphi(6)}$
$5^23 \equiv 5^1 \equiv 5 \pmod{6}$

**3 pass-protocol**

- Physical world version:

  Alice want to mail Bob a box through the mail, Alice takes the box and puts her lock on it, mails it to Bob, Bob locks the box again with his lock, Alice removes her lock, Bob unlocks the box and retrieve whats inside.

- Math version:

  Message is encoded as a number, Alice pick a large prime number P(not secret), Alice picks a secret number a coprime to p-1, Bob picks a secret number b coprime to p-1, Eve encrypts m with $E_A(\text{m}) = m^a(\text{mod p})$,

  Eve computes $a^{-1}$(mod p-1)

  Bob computes $b' \equiv b^{-1}$(mod p-1)

  $D_A(\text{C}) \equiv C^{a'}(\text{mod p})$

  $\text{C} = E_A(\text{m}) \equiv m^a(\text{m mod p})$

  $D_A(\text{C}) = C^{a'}(\text{m mod p})$

  $= (m^a)^{a'} \text{ (mod p)}$

  $= m^{aa'} \text{ (mod p)}$

  $= m^{\ell(p-1)+r} \text{ (mod p)}$

  $= (m^{p-1})^{\ell} \text{ m (mod p)}$

  $= \text{m (mod p)}$

- Math version of 3 pass protocol

  Alice computes $C_1 \equiv m^a \text{ (mod p)}$

  sends to bob

  Bob computes $C_2 \equiv C_2^a \text{ (mod p)}$

  sends to Alice

  she raises to the $a'$ power

  $C_3 \equiv C_2^{a'} \text{ (mod p)}$

  Bob computes $C_4 \equiv C_3^{b'} \text{ (mod p)}$

  $C_4 \equiv C_3^{b'} \equiv (C_2^{a'})^{b'} \equiv ((C_1^b)^{a'})^{b'} \equiv (((m^a)^b)^{a'})^{b'}$

  $\equiv m^{aba'b'} \text{ (mod p)}$

  $\equiv m \text{ (mod p)}$