MATH 314 Fall 2019 - Class Notes

09/23/2019

Scribe: Sujan Tulachan

Summary: We worked on basics principle of fermat's little theorem, 3 Pass protocol, and Euler Phi Function

Notes: when doing arithmetic (mod p). we reduce exponent (mod p-1)
Example:

$x^3 \equiv 6 \pmod{11}$
raise both sides to power a
$x^{3a} \equiv 6^a \pmod{11}$
Goal is to find a when 3a $\equiv 1 \pmod{10}$
$10 = 3 * 3 + 1$
$3 = 3 * 1 + 0$
$1 = 10 - 3 * 3$
$1 \equiv -3 * 3 \pmod{10}$
$3^{-1} \equiv 7 \pmod{10}$

$x^{3*7} \equiv 6^7 \pmod{11}$
$x^{21} = x^{10^2} \equiv 6^7 \pmod{11}$
$1 * x \equiv 6^7 \pmod{11}$
$x \equiv 6^4 * 6^2 * 6 \pmod{11}$
Note
$6^2 \equiv 36 \equiv 3 \pmod{11}$
$6^4 \equiv 3^2 \equiv 9 \pmod{11}$
$x \equiv 4 * 3 * 6 \pmod{11}$
$x \equiv 8 \pmod{11}$

3-Pass Protocol

Physical Version
Alice want to send the mail package to bob. Alice put lock without the key to Bob. Then, Bob again put the lock without key and sends back to Alice. Alice unlock her lock and sends back to Bob. Then finally, bob unlock his key and retrieves

the message.

Math Version

Alice is going to pick big prime number p(usually 200 digits)
Alice can tell everyone about p)
Then, She picks a random secret number a where 0<a<p-1) and gcd(a,p-1)=1

Alice's Encryption Function)

E(x)$\equiv$ x$^a \pmod p$

Alice's Decryption Function
D(y)$\equiv$y$^{a^{-1}} \pmod p$

Bob also picks a secret number b where b is 0<b<p-1 where gcd(b,p-1)= 1
he also computes b^{-1}
Note:
b^{-1} exists only if gcd(b, p-1)=1
Alice takes the plaintext and encodes it as a number m such that 0$\leq$m<p
She computes C1 $\equiv$ E(m) $\equiv m^a \pmod p$
She sends C1 to Bob

Bob encrypts C1
She computes C2 $\equiv$ E(c1) $\equiv c1^b \pmod p$

He sends C2 back to Alice
She decrypts C2

She computes C3 $\equiv$ D(c2) $\equiv c2^{a^{-1}} \pmod p$

She sends C3 back to Bob
He computes C4 $\equiv$ D(c3) $\equiv c3^{b^{-1}} \pmod p$
C4 $\equiv m^{a*b*a^{-1}*b^{-1}}$
C4 $\equiv m \pmod p$

Drawback
Have to send 3 different messages
Man in the middle attack works well against the 3- pass Protocol

Euler Phi Function

$\varphi(n) =$ no of integer a in 1≤a<n with gcd(a,n)= 1
Examples:
$\varphi(12) = 4$
$\varphi(26) = 12$
$\varphi(11) = 10$

if 'p' is a prime then
$\varphi(p) = p - 1$
$\varphi(p^k) = p^{k-1}(p-1)$

if the gcd(a,b)=1 $\varphi(ab) = \varphi(a) * \varphi(b)$
Examples:
$\varphi(24) = \varphi(8 * 3)$
$\varphi(2^3 * 3) = \varphi(2^3) * \varphi(3)$
$2^2(2-1) * (3-1) = 8$
Therefore, there are 8 numbers between 1 and 24 that doesn't have common factor with 24

$\varphi(700) = \varphi(7 * 100)$
$\varphi(2^2 * 5^2) * (7) = \varphi(2^2) * \varphi(5^2) * \varphi(7)$
$6 * 2 * 20 = 8$

Euler's Theorem if gcd(a,n)=1 then $a^{\varphi(n)} \equiv 1 \pmod{n}$

Basic Principle for exponents (mod n). if working in (mod n) then we work mod $\varphi(n)$ in the exponents.