MATH 314 Spring 2018 - Class Notes

11/24/2018

Alec Totushek

Summary: In class we learned about multiple mathematical theorems and techniques–namely The Chinese Remainder Theorem, residues, Euler's Totient Function, Euler's Theorem, and finite fields–in order to make progress towards a cryptosystem that is simpler than, but has the same security as the 3-pass protocol

Notes:

Chinese Remainder Theorem: If we have 2 numbers m and n where $gcd(m, n) = 1$, then the equations $X \equiv a(mod\ m)$ and $X \equiv b(mod\ n)$ have a unique solution modulo $m * n$

Example 1:

$m = 2$; $n = 13$
$X \equiv 1(mod\ 2)$; $X \equiv 8(mod\ 13)$
$13+8=21$
$21(mod\ 13) = 8$; $21(mod\ 2) = 1$
$X = 21$

Co-Prime Numbers: If two numbers m and n have $gcd(m,n) = 1$, we say they are coprime.

Residues: Each of the possible remainders of a number modulo n is called a residue *(mod n)*.

Example 2:

$X \equiv 3(mod\ 7)$; $X \equiv 12(mod\ 13)$
We need to find the residue *(mod m*n)* ; $m*n = 91$.
The first equation tells us $X = 3 + 7k$ where $7k$ is a multiple of 7.
Next, find *gcd(7,13)* and use the extended Euclidian algorithm to find 7^{-1}:
$13 = 7(1) + 6$; $7 = 6(1) + 1$; $6 = 1(6) + 0$
$1 = 7 + 6(-1) = 7 + (13 + 7(1))(-1) = 7(2) + 13(-1)$
$7^{-1} = 2$
Now find k:
$3 + 7k = 12(mod\ 13)$; $7k = 9(mod\ 13)$; $k = 18(mod\ 13)$; $k \equiv 5(mod\ 13)$
Now use k to find $X(mod\ 91)$:
$X = 3 + 7(5) = 3 + 35 = 38 \equiv 38(mod\ 91)$

.

Euler's Totient Function/Phi Function: $\phi(n)$ counts how many residues *(mod n)* are co-prime to n.

- $\phi(n) = n\Pi(\frac{p-1}{p})$ for all prime factors p *of* n
- If p is prime and $n = p$, then $\phi(n) = p - 1$
- If p,q are prime, then $\phi(p*q) = (p - 1)(q - 1)$

Example 3

$\phi(60)$
Primes that divide 60: *2, 3, 5*
$\phi(60) = 60(\frac{1}{2})(\frac{2}{3})(\frac{4}{5}) = 16$

Euler's Theorem: If a number a is co-prime to n, then $a^{\phi(n)} \equiv 1$*(mod n)*

- We can relate this theorem to Fermat's little theorem if n is prime:
  - if $n = p$, then $a^{\phi(p)} = a^{p-1}$, which is Fermat's little theorem

In General, when doing exponential arithmetic *(mod n)*, all that matters is the result *(mod* $\phi(n)$*)*

Example 4

4^{10}*(mod 15)*
$\phi(15) = 8$; therefore, $4^8 = 1$*(mod 15)*
4^{10}*(mod 15)* $= 4^8 * 4^2$*(mod 15)* $\equiv 1 * 16$*(mod 15)* $\equiv 1$*(mod 15)*

Fields: If we have a collection of things that we can apply all basic arithmetic operators to by anything other than 0 while staying inside of the collection, we call this a field.

- $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Q}$ are all fields

Finite Field: a field with a finite amount of elements

- Denoted $\mathbb{F}_q$ for a finite field with q elements
- If q is prime, then $\mathbb{F}_p$ is the set of residues *(mod p)*
- If q is composite, then $\mathbb{F}_q$ is not the set of residues *(mod q)*

Example 5

Is $\mathbb{F}_4$ a finite field?
Test for ever element *[0,3]* under addition, subtraction, multiplication, and division *(mod 4)*
When texting for multiplication, we see that in row 2 we get: (products in bold)
$*$ — *0* — *1* — *2* — *3*
2 — ***0*** — ***2*** — ***0*** — ***2***
Since row 2 has no inverse, $\mathbb{F}_4$ cannot be a field under division, therefore $\mathbb{F}_4$ is not a finite field.