MATH 314 Spring 2018 - Class Notes

2/26/2019

Scribe: Caitlin Nanashko

Summary: Today's class covered the Chinese Remainder Theorem

Notes: Chinese Remainder Theorem (CRT)

- If m and n are coprime ($gcd(m, n) = 1$) then the equations $x \equiv a(modm)$ and $x \equiv b(modn)$ have a unique solution (mod mn) for any a + b

Example 1: `Find a solution to` $x \equiv 3(mod7)$ `and` $x \equiv 12(mod13)$.
CRT says there is a solution (mod 91)

$x \equiv 3(mod7)$ means x = 3 + 7k for some integer k

plug this into $x \equiv 12(mod13)$

$$3 + 7k \equiv 12(mod13)$$

$$7k \equiv 9(mod13)$$

Need $7^{-1}(mod13)$

$$7^{-1} \equiv 2(mod13)$$

$$2(7k) \equiv 2(9)(mod13)$$

$$k \equiv 18(mod13)$$

$$k \equiv 5(mod13)$$

- If n = ab where gcd(a,b) = 1 then if x(mod n) is invertible and x(mod a) and x(mod b) are invertible

φ is greek letter phi you could also see it as ϕ

- Using the CRT we can take any invertible residue (mod a) and one (modb) and find a unique solution to both (mod n) that is also invertible

$\varphi(a)$ invertible residue (mod a)

$\varphi(b)$ invertible residue (mod b)

$\varphi(n) = \varphi(a)\varphi(b)$ if n = ab and gcd(a,b) = 1

$\varphi(25) = \frac{4}{5}(25) = 4 * 5 = 20$

$\varphi(125) = (5^3) = \frac{4}{5}(125) = 4 * 25 = 100$

$\varphi(p^2) = \frac{p-1}{p}(p^2)$

$$\varphi(120) = \varphi(5) * \varphi(24)$$
$$= \varphi(5) * \varphi(3) * \varphi(2^3) = (5-1)(3-1)(2-1)(2^2)$$
$$= (4)(2)(1)(2^2) = 32$$

Fuler's Theorem: `if a is coprime to n then` $a^{\varphi(n)} \equiv 1$ (modn)

Note: `if n = p is prime then` $\varphi(p) = p - 1 \;\; a^{p-1} \equiv 1(modp)$

Example: `Compute` $7^{17}(mod 15)$
`Use Eucler's Theorem` $\varphi(15) = \varphi(3)\varphi(5) = (3-1)(5-1) = 8$

$$= 7^8 \equiv 1(mod 15$$
$$7^{17} \equiv 7^8 * 7^8 * 7^1 \equiv 7(mod 15)$$

In a ring we can add, subtract, and multiply, but we can't always divide

Sometimes we have a ring where we can divide by everything except 0 these are **fields**.

Important fact about fields: there is at most one finite field with n elements for any n.