MATH 314 Spring 2018 - Class Notes

03/05/2019

Scribe: Michael Quang

Summary: Today's class covered Primitive Roots, Quadratic Residues, and Legendre Symbols.

Notes: If the powers of a(mod p) doesn't reappear before the pth power equivalently every residue appears as a power of a(mod p) we call a a primitive residue (mod p) or primitive root.

Important fact: If a is a primitive root and $a^k \equiv a^l$ (mod p) then k $\equiv$ l (mod p-1)

Definition: If $x^2 \equiv a$ (mod p) has a solution we call a a quadratic residue if it doesn't have a solution it is called a quadratic nonresidue.

Define Legendre Symbol $\left(\dfrac{a}{p}\right)$ "a on p"

1. 0 if p/a
2. 1 if $x^2 \equiv a$ (mod p) exists
3. -1 if it has no solution
   Note: The bottom number of a Legendre Symbol has to be an odd prime

Rules for Legendre Symbols

1. $\left(\dfrac{a}{p}\right) = \left(\dfrac{b}{p}\right)$ if a $\equiv$ b (mod p)
2. $\left(\dfrac{ab}{p}\right) = \left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$
3. Quadratic Reciprocity
   If p and q are both odd primes $\left(\dfrac{p}{q}\right) = \left(\dfrac{q}{p}\right)$ unless both p $\equiv$ 3 (mod 4) and q $\equiv$ 3 (mod 4)
   $\left(\dfrac{p}{q}\right) = -\left(\dfrac{q}{p}\right)$ if p $\equiv$ q $\equiv$ 3 (mod 4)
4. $\left(\dfrac{2}{p}\right)$ = 1 if p $\equiv$ 1 or 7 (mod 8) or -1 if $\equiv$ 3 or 5 (mod 8)

5. $\left(\dfrac{1}{p}\right) = 1$

Example 1: Find inverse of x^2+1 on the field $\mathbb{F}_{32}$(mod x^5+x^3+1)

$$\begin{gathered} x^2+1/x^5+x^3+1 = x^3R1 \\ x^5+x^3+1 = x^3(x^2+1) \\ 1 = (x^5+x^3+1)+x^3(x^2) \\ 1 \equiv x^3(x^2+1) \text{ (mod } x^5+x^3\text{+1)} \\ (x^2+1)^{-1} \equiv x^3 \text{ (mod } x^5\text{+}x^3\text{+1)} \end{gathered}$$

Example 2: Find inverse of x^2+x+1 (mod x^5+x^3+1)

$$\begin{gathered} x^2+x+1/x^5+x^3+1 = x^3+x^2+x \text{ R(x+1)} \\ x^5+x^3+1 = (x^3+x^2+x)(x^2+x+1)+(x+1) \\ (x^2+x+1) = x(x+1)+1 \\ (x+1) = (x^5+x^3+1)+(x^3+x^2+x)(x^2+x+1) \\ 1 = 1(x^2+x+1)+x((x^5+x^3+1)+(x^3+x^2+x)(x^2+x+1)) \\ 1 = x(x^5+x^3+1)+(x^4+x^3+x^2+1)(x^2+x+1) \\ 1 \equiv (x^4+x^3+x^2+1)(x^2+x+1)(modx^5+x^3+1) \\ (x^2+x+1)^{-1} \equiv x^4+x^3+x^2+1 \end{gathered}$$

Example 3: For what values of a does $x^2 \equiv a$ (mod p) have a solution?

a = 1, 3, 4, 5, 9

$x^2 \equiv 2$ (mod 11) has no solution (no x works)

Example 4: Is 42 a square mod 31?

$$\left(\frac{42}{31}\right) = \left(\frac{11}{31}\right) = \text{-}\left(\frac{31}{11}\right) = \text{-}\left(\frac{9}{11}\right) = \text{-}\left(\frac{3}{11}\right)\left(\frac{3}{11}\right) = \text{-(1)(1) = -1}$$

$$\left(\frac{3}{11}\right) = \text{-}\left(\frac{11}{3}\right) = \text{-}\left(\frac{2}{3}\right) = \text{-(-1) = 1}$$