MATH 314 Spring 2018 - Class Notes

3/6/2018

Scribe: Isaac Tray

Summary: Today in class, we discussed quadratic residues, the legendre symbol, it's rules and an example. As well as the jacobi symbol, it's rules.

Notes: Quadratic Residue

Definition: If $x^2 \equiv b(modp)$ has a solution, we call 'b' a quadratic residue (mod p). If it does not have a solution, we call 'b' a quadratic nonresidue.

Legendre Symbol:

Legendre Symbol: $(\frac{a}{p})$

Note: Prononced "a on p", and for the legendre symbol, 'p' must be prime

Legendre Symbol Solutions:

1. 0, if a $\equiv$ 0(mod p)
2. 1, if $x^2 \equiv$ a(mod p) has a solution
3. -1, if $x^2 \equiv$ a(mod p) has no solution

Legendre Symbol Rules:

1. If a $\equiv$ b(mod p) then $(\frac{a}{p}) = (\frac{p}{a})$
2. $(\frac{1}{p}) = 1$
3. $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$
4. Quadratic Reciprocity: if p and q are both primes, then $(\frac{q}{p}) = -(\frac{p}{q})$ if p $\equiv$3(mod 4) and q $\equiv$ 3(mod 4)
5. $(\frac{2}{p})$ is -1 if p = 3 or 5(mod 8) or is 1 if p = 1 or 7(mod 8)

Legendre Symbol Example: Is 11 a square (mod 43)?

$(\frac{11}{43})$ = -$(\frac{43}{11})$ (By Rule 1)

= -$(\frac{10}{11})$ (Because 43 = 10(mod 11))

= -$(\frac{2}{11})(\frac{5}{11}) = (\frac{5}{11})$ (Because -$(\frac{2}{11})$ = -1)

$(\frac{5}{11}) = (\frac{11}{5}) = (\frac{1}{5}) = 1$

Because the final answer is 1, 11 is a square (mod 43)

Jacobi Symbols:
Like Legendre symbols but the number on the bottom can be composite. Note: If $(\frac{n}{m}) = 1$, does not mean n is a square mod m. If the Legendre symbol and Jacobi symbol are both defined they are equal.

Jacobi Symbol Rules:

1. If a $\equiv$ b(mod n) then $(\frac{a}{n}) = (\frac{b}{a})$
2. $(\frac{1}{n}) = 1$
3. $(\frac{2a}{n}) = (\frac{2}{n})(\frac{a}{n})$
4. If n and m are odd, then $(\frac{n}{m}) = -(\frac{m}{n})$ if n and m $\equiv$3(mod 4) otherwise $(\frac{m}{n})$
5. $(\frac{2}{n})$ is -1 if p = 3 or 5(mod 8) or is 1 if p = 1 or 7(mod 8)