MATH 314 - Class Notes

10/3/17

Scribe: Jorge Luis Brito

Summary: The Legendre symbol and Jacobi Symbols.

Notes: We worked on some Legendre and Jacobi symbol problems and then did a worksheet

Definition: The Legendre Symbol

(a/p)

- 1 if a is a quadratic residue (mod p)
- 0 if a equivalent 0(mod p)
- -1 if a is not a quadratic residue mod p

Legendre Symbol Facts

1. (a/p) = (b/p) if a equivalent b(mod p)
2. ab/p = (a/p)(b/p)
3. (2/p)=
   - 1 if p=1 or 7 (mod 8)
   - -1 if p=3 or 5 (mod 8)
4. If p and q are both odd primes then (q/p)=
   - -(p/q): if p equivalent to q and q equivalent to 3 (mod 4)
   - (p/q): otherwise

Lengendre Example

Is 1001 a square mod 9907?

1001 = 7 x 11 x 13

$\frac{1001}{9907} = \frac{7}{9907}x\frac{11}{9907}x\frac{13}{9907} = 1$

$\frac{7}{9907} = -\frac{7}{9907}$

$\frac{-2}{7} = 1$

$9907 = 2(mod 7)$

Jacobi Symbol

Suppose n = $p_1^{e_1} p_2^{e_2} p_k^{e_r}$

Definition: Jacobi Symbol

a/n= $(\frac{a}{p_1})^{e_1}(\frac{a}{p_2})^{e_2}...(\frac{a}{p_k})^{e_r}$
Bottom of a Jacobi symbol doesn't nee to be a prime but if H is the the Jacobi symbol is the same as the Legendre symbol.

Can't use Jacobi symbol to tell if a is a quadradic residue mod m

Example: Jacobi Symbol

$\frac{8}{15} = 1$ but 8 is not a square(mod 15)
Rules for Jacobi Symbol

- $\frac{a}{n} = \frac{b}{n}$ if a $\equiv b(mod n)$
- $\frac{2}{n} =$
  1. 1 if n is 1 or 7(mod 8)
  2. -1 if n is 3 or 5 (mod 8)

  1. 1 if n is 1 or 7(mod 8)
  2. -1 if n is 3 or 5 (mod 8)

if a is odd
$\frac{a}{n} =$

- $-\frac{n}{a}$ if $a \equiv n \equiv 3(mod 4)$
- $\frac{n}{a}$ otherwise.

using these rules we can compute that $\frac{a}{n}$ for any numbers a, n without having to factor either **a** or **r**

$\frac{1001}{9907}$ Using Jacobi Symbols

$\frac{1001}{9907} = \frac{9907}{1001} = \frac{898}{1001} = \frac{2}{1001} = -\frac{1001}{449} = \frac{449}{103} = \frac{37}{103} = \frac{103}{37} = \frac{29}{37} = \frac{37}{29}\ \frac{8}{29} = (\frac{2^3}{29})$ x$(\frac{2^3}{29})$x$(\frac{2^3}{29})$

(-1)x(-1)x$(-1) = -1$
$= \frac{2^3}{29} = \frac{103}{449}(\frac{449}{1001}) = 9907 \equiv 898(mod 1001)$

using these rules we can compute that $\frac{a}{n}$ for any numbers a, n without having to factor either a or