Notes 9/30

Kristen Thesing

October 21, 2019

-a is a primitive root mod p if a^k
produces all the numbers 1,2..p-1 as k varies from 1 top
-The powers of a are all the residues (mod p) besides 0
-Every prime number has atleast one primitive root
-ex: Primitive roots(mod 11) are 2,6,7,8
-if $a^x \equiv a^y \pmod{p} then x \equiv y \pmod{p-1}$
-in the example 1,4,9,5,3 have square roots(mod 11)
-$x^2 \equiv 6 \pmod{11} has no solution$
-a is a quadratic residue if $x^2 \equiv a \pmod{p}$
has a solution
-if a is NOT a quadratic residue we call it quadradic
non-residue
-for a prime number p
(a/p) = 1 if $x^2 \equiv a \pmod{p}$
0 if a$\equiv 0 \pmod{p}$
-1 if $x^2 \equiv a \pmod{p} has no solution$
Note: Number on bottom is prime
ex: (4/11) = 1 because 4 was a quadratic residue and has a
square root
ex: (6/11) = -1 b/c is not in the list of square roots
ex:(10/11) = -1 b/c is not in the list of square roots
ex:(22/11) = 0 because 0$\equiv 22 \pmod{11}$
ex: (16/11) = (5/11) = 1 b/c it is in the square roots
Rules for Legendre Symbol
(a/p) = (b/p) if a $\pmod{p}$
-(ab/p) = (a/p)(b/p)
-quadratic reciprocity: if p and q are both odd primes
then (q/p)= -(q/p) if p= q$\equiv 3 \pmod{4}$
(p/q) otherwise
-(2/p) = 1 if p$\equiv 1, 7 \pmod{8}$
-1 if p$\equiv 3, 5 \pmod{8}$
-(1/p) = 1
ex: is 43 a quadratic residue(mod 73)?
(43/73) -> (73/43) = (30/43) = (2/43)(3/43)(5/43)

(3/43) = -(43/3) = -(1/3) = -1
(5/43) = (43/5) = (3/5) = (5/3) = (2/3) =-1
ex: (1001/9907) =(7/9907)(11/9907)(13/9907)
=(9908/7)*(9907/11)*(9907/13)
=-(2/7)*(-7/11)*(1/13)
=1
$2_{\frac{}{3}}$