MATH 314 - Class Notes

09/28/2017

Scribe: Sundeep Singh

Summary: Introduction to finite fields, Primitive roots, Legendre Symbols, and Quadratic residues

Notes: 28 September 2017

$\mathbb{F}_4$(Field with 4 elements)

Polynomials $\mathbb{F}_2[x]$ modulo $x^2 + x + 1$

$x^3 + x + 1$ is also irreducible

Look at Polynomials modulo $x^3 + x + 1$

There are 8 residuals modulo $x^3 + x + 1$

These residues will form a field $\mathbb{F}_8$

Important

Fact for every n¿= 1 there exists an irreducible polynomial in F2[x] of degree n.

The field F_{2^n} is obtained by taking the polynomials $\mathbb{F}_2[x]$ modulo $g(x)$ where $g(x)$ has is irreducible and has degree n.

Definition

A primitive root (mod p) is a residue a such that the powers $a, a^2, a^3, ---, a^(p-1)$ (don't repeat), include every residue (mod p)

Primitive root

If a is a primitive root (mod p) then for any other residue $b \neq 0$.

There is some power i so that a^i is equivalent to b(mod p)

Every prime p has at least one primitive root.

If g is a primitive root and g^i equivalent g^j(mod p).Then i equivalent j (mod $p-1$).

Definition

If a(mod p) has a square root meaning x^2 equivalent a(mod p) has a solution then we call a a quadratic residue (mod p). If not we call a a quadratic non-residue.

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

Example: Is 1001 a quadratic residue mod 9907?

$1001 = 7 \times 11 \times 13$
(1001/9907) $=$ (7/9907) $\times$ (11/9907) $\times$ (13/9907) $= 1$
(7/9907)=-(9907/7)
-(9907/7)=-(2/7)
(-2/7)=-1
$9907 = 2(mod 7)$