2/26/18 Class Notes

Manish Joshi

March 9, 2018

When we are doing arithmetic modulo a prime number p, every residue besides 0 is inversible. This means that we can divide by everything except 0.

Field -A ring where it is possible to divide by any element except 0 is called a field. Ex- Real numbers R ,Rational numbers Q, Arithmetic modulo a prime number 'p' F_p

1 Finite Field

We call a field like F_p with finitely many things in it a Finite Field. If n=p is prime then, F_p is the integers mod p. If n is not prime then F_n is not the integers mod n. For example, Consider, n = 4. Write down the addition and multiplication table mod 4.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

X	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

1.1 Polynomials

Let $F_2[2]$ be the collection of polynomial whose coefficients are elements of $F_2[2]$ (0 or 1).

Example: g(x)= $x^3 + x + 1$ (g(x) is in F_2)

If f and g are two polynomials in F_2[x], we can add them:

g(x)= $x^3 + x + 1$

f(x)= $x^2 + x$

g(x)+ f(x) = $x^3 + x^2 + 1$ (x+x = 2x which is 0x mod 2)

Note: Addition and Substraction are the same in F_2[x].

f(x) $\cdot$ g(x) = $(x^2 + x)(x^3 + x + 1)$
=$(x^5 + x^3 + x^2) + (x^4 + x^2 + x)$
=$x^5 + x^4 + x^3 + x$

So, F2[x] is a ring.

Even though we can't divide any two polynomials in F2[x], we can do division with remainder. So, the remainder should have degree smaller than the quotient.

$x^3 + x + 1/x^2 + x$ is x+1 remainder 1.
g(x)= $x^3 + x + 1 \equiv 1(mod x^2 + x)$

F2[x]- irreducible polynomial p(x) of degree n.
Say that p(x) <- F2[x] is rreducible if it cannot be evenly divided by any polynomial of smaller degree besides 1.
Arithmetic in $F_2[x]$ modulo p(x) F_{2^n}.
Example:
Construct F_4.

$F_4 = F_{2^2}$.
Claim: $x^2 + x + 1$ is irreducible in $F_2[x]$.
What are the polynomials of smaller degree?
$x, x + 1$

$x^2 + x + 1/x$ is x+1 remainder 1.
$x^2 + x + 1/x + 1$ is x remainder 1.

So, arithmetic mod $x^2 + x + 1$ is a field.
Possible remainders are $\{x, x + 1, 1, 0\} = F_4$.

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

X	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	0

Note: Everything in F_4 is invertible other than 0.