MATH 314 - Class Notes

3/7/2017

Scribe: Jacob Lee

Summary: This set of notes will cover Finite Fields, Modular Arithmetic with Polynomials, and Quadratic Residues.

Notes:

1 Some useful facts to start

- Every prime has at least two primitive roots
- If g is a primitive root (mod p) then: $g^n \equiv 1$ **IFF** n is a multiple of p - 1
- If $g^i \equiv g^3(\text{mod } p)$, then $i \equiv j(\text{mod } p$ - 1)

2 Finite Fields

If p is prime, then $\mathbb{F}_p$ is the Finite Field with p elements. (This is the integers modulo p)

If n is **composite**, then $\mathbb{F}_n$ is **not** the integers modulo n

Example: $n = 4$

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

Here we can see that 2 (row **2** containing values **0, 2, 0, 2**) does not have an inverse modulo 4, so $n = 4$ is **not** a field.

3 Polynomials with Coefficients in $\mathbb{F}_2$($\mathbb{F}_2$[x])

We can do addition, subtraction, and mulitplication pretty simply, but division is slightly harder so we'll start with that.
Example: Division with a remainder: $x^2 + x + 1 \overline{)x^3 + 0x^2 + x + 1}$

After doing the some polynomial long division we get: x+1 R x
Thus, we can say that $f(\text{x}) = x^2 + x + 1$ is "smaller" than $g(\text{x}) = x^3 + 0x^2 + x + 1$ if the degree(highest power of x) in $f(\text{x})$ is less than the degree of $g(\text{x})$.

4 Modular Arithmetic with Polynomials

Say that f(x) $\equiv g$(x)(mod m(x)).

If the remaindeer when dividing f(x) by m(x) is the same as the remaindr when dividing g(x) by m(x) then...
Using the example of polynomial division from the previous section...

$$x^3 + x + 1 \equiv x(mod x^2 + x + 1) \text{ in } \mathbb{F}_2[x]$$

5 Comparisons

Z ring $\mathbb{F}_2[x]_{m(x)}$ modulo

$Z\ mod_{p-prime}P$ Field $\mathbb{F}_p[x]_{g(x)}$ modulo, where $g(x)$ is irreducable.

Irreducable meaning: if not divisable with remainder 0 by any polynomial with degree smaller than the $g(x)$ besides 1

Polynomials in $\mathbb{F}_2[x]$ of Small Degree

Degree = 0:
0, 1

Degree = 1:
$x + 0, \quad x, \quad x + 1$

Degree = 2:
$x^2, \quad x^2 + 1, \quad x^2 + x + 1$

Claim: $x^2 + x + 1$ is irreducable

Check: $x \overline{)x^2 + x + 1} = x^2 + 1\ R\ 1$

Check: $x + 1 \overline{)x^2 + x + 1} = x\ R\ 1$

This tells us that $\mathbb{F}_2[x]$ (mod$x^2 + x + 1$) should be a field!

So possible residues in this field are 0, 1, x, $x + 1$

SO... all polynomials in $\mathbb{F}_2[x]$ of degree smaller than $x^2 + x + 1$

6 Polynomial Addition and Multiplication

Addtion

+	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

Multiplication

*	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	1	$x+1$	1
$x+1$	0	$x+1$	1	x

This has 4 elements so this $\mathbb{F}_4$

Working modulo x^2+x+1 produced $\mathbb{F}_4$

If we wanted $\mathbb{F}_{2^n}$, we can work with polynomials in $\mathbb{F}_2[x]$ modulo $q(x)$; where $q(x)$ is reducable of degree n.

x^3+x+1 is irreducable so $\mathbb{F}_8[x]$ is $\mathbb{F}_2 \pmod{x^3+x+1}$

In general $\mathbb{F}_{p^n}$ is $\mathbb{F}_p[x]$ (mod ***some irreducable polynomial of degree*** n*)

7 Quadratic Residues

Say a **is** a **quadratic residue** $\pmod p$ if $x \equiv a \pmod p$ has a solution.

Say it's a **quadratic non-residue** if it does **not**.

Example: $p = 7$

a	$a^2 (mod 7)$
1	1
2	4
3	2
4	2
5	4
6	1

Here we can see that 1, 4, 2 are quadratic residues and 3, 5, 6 are quadratic non-residues.

If p is an **odd** then there are $\frac{(p-1)}{2}$ quadratic residues as well as $\frac{(p-1)}{2}$ quadratic non-residues.

If p is an odd prime then a is a quadratic residue.

If $a^{(p-1)/2} \equiv 1 \pmod{p}$ we get a residue
If $a^{(p-1)/2} \equiv -1 \pmod{p}$ we get a non-residue