MATH 314 - Class Notes

10/4/2016

Scribe: Tyler Howard

Summary: Reviewed content for Midterm 1. Covered primitive roots, quadratic residues, and continued looking at arithmetic with finite fields.

Notes: Midterm 1 has been completed, therefore only new material will be covered in these notes.

What is a primitive root modulo p?

- Let g be a primitive root (mod p) where p is prime.
- Then g^1, g^2, g^3, g^{p-1} are all of the nonzero remainders mod p

Facts about primitive roots to note:

- If g is a primitive root mod p, then
  1. $g^n = 1 mod p$ if and only if n is a multiple of $p-1$ ie $n = 0 mod(p-1)$
  2. If $g^i \equiv g^j mod p$ then $i \equiv j mod p - 1$

What is a quadratic residue (mod p)?

- a is a quadratic residue mod p, where p is prime, if $x^2 \equiv a mod p$ has a solution
- Example:
  - Residues $mod 7 = 1, 2, 3, 4, 5, 6$
  - Squared residues $mod 7 = 1^2, 2^2, 3^2, 4^2, 5^2, 6^2 \equiv 4, 2, 2, 4, 1$
  - So: 1, 2, and 4 are quadratic residues (mod 7) and 3, 5, 6 are not.

Finite Fields

- A field with n elements is a finite field, we write $\mathbb{F}_n$ to denote it
- Remember, if n is prime then $\mathbb{F}_p$ is the integers mod p
- If it is not prime then $\mathbb{F}_n$ is the integers mod n

Recall last time: Polynomials with coefficients in $\mathbb{F}_2$

- Add, subtract, multiply these polynomials
- So these polynomials form a ring, like the set Integers
- Division with remainder in $\mathbb{F}_2$[x] example:
  $x^2 + x + 1\overline{)x^3 + 0x^2 + x + 1}$
  $= x + 1$ remainder: x

- Using this characteristic of fields, we can do modular arithmetic of polynomials in $\mathbb{F}_2$[x] modulo another polynomial.

Big example of polynomial arithmetic within $\mathbb{F}_2$.

- $x^3 + x + 1 mod(x^2 + x + 1) \equiv x mod(x^2 + x + 1)$
- Notice the similarities:
  Integers $\Leftrightarrow$ Polynomials with coefficients in $\mathbb{F}_2$
  Integers modulo n $\Leftrightarrow$ Polynomials modulo $\mathbb{F}$[x]
  Integers modulo p (finite) $\Leftrightarrow$ Polynomials modulo P[x](irreducible,prime)

Claim: $x^2 + x + 1$ is prime in $\mathbb{F}_2$

- Are they any polynomials smaller than $x^2 + x + 1$ in $\mathbb{F}_2$?
- Yes, we find $x + 1, x, 1, and 0$. Zero is negligible in this case.
- Lets check if prime: $x + 1\overline{)x^2 + x + 1} \equiv x remainder 1$
- So we find that the polynomial $x^2 + x + 1$ behaves like a prime in $\mathbb{F}_2$

Since $x^2 + x + 1$ is irreducible, the polynomials modulo $x^2 + x + 1$ should be a field.

Addition table modulo $x^2 + x + 1$

+	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 table modulo $x^2 + x + 1$

+	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	x

Notice that $x * x = x^2$ which is not possible modulo $x^2 + x + 1$. Instead we must take the the inverse of $x \equiv x + 1$. Likewise $x + 1 * x + 1$ requires the inverse of $x + 1 \equiv x$

So, $x^3 + x + 1$ is irreducible too.
This is $\mathbb{F}_4$, because there is 4 residues in the set.
Similarly, if you take polynomials modulo $x^3 + x + 1$, you get a field with 8 possible remainders.

Therefore, you get $\mathbb{F}_8$.