MATH 314 Spring 2018 - Class Notes

02/27/2018

Scribe: Brian Roshal

Summary: Today in class, we covered Finite Fields and polynomials over finite fields.

Notes: If we are doing modular arithmetic modulo a prime number p, then every residue besides 0 is invertible.

Recall: a ring is a set of things that can be added, subtracted, multiplies (sometimes, divided).

Ex: Integers, Rational numbers, Real numbers, Integers mod n, Complex numbers, Square matrices, and Polynomials.

Definition: a ring where every element is invertible besides 0 is called a field.

Rational Numbers: $\mathbb{Q}$
Real Numbers: $\mathbb{R}$
Complex Numbers: $\mathbb{C}$
Integers modulo p, p is prime:

We call a field with finitely many things in it a Finite Field

Fact: For any integer n, there exists at most one field with exactly n elements in it. If it exists, we call is $\mathbb{F}_n$

Note: If n is not prime, then $\mathbb{F}_n$
is not the integer mod n.

+	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

The row of 2 is not a field because 2 is not invertible

Start with $\mathbb{F}_2$[x], this is the set of all polynomials with coefficients in $\mathbb{F}_2$.
Ex: $g(x) = x^3 + x + 1$
$f(x) = x^2 + x$

Compute $f(x) + g(x)$
$f(x) + g(x) = x^3 + x^2 + 2x + 1 \ = x^3 + x^2 + 1$
In this example, mod=2, multiplying by 2 is equivalent to multiplying by 0.

Weird fact: in $\mathbb{F}_2$[x], addition and subtraction are the same thing. $f(x)+g(x) = f(x)-g(x)$

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

So $\mathbb{F}_2$[x] is a ring, even though we can't do division, we can still do division with remainder.

We want the remainder to be a polynomial who's size and degree is smaller than the quotient.

Divide $g(x)$ by $f(x)$ with remainder
$(x^3 + x + 1)/(x^2 + x) = x + 1R1$
$x^3 + x + 1 \equiv 1(\text{mod } x^2 + x)$

Ring: Integers modulo a prime number $p \to$ Field $\mathbb{F}_\mathrm{p}$
Ring: Polynomials mod 2 modulo an irreducible polynomial $p(x)$ of degree $n \to$ Field $\mathbb{F}_{2^\mathrm{n}}$ arithmetic mod 2.

Say $p(x) \in \mathbb{F}_2[x]$ is irreducible, if the only polynomial of smaller degree that evenly divides it is 1. Let's find $\mathbb{F}_4$
Claim that $p(x) = x^2 + x + 1$ is irreducible

Check $(x^2 + x + 1)/(x) = x + 1R1$ $(x^2 + x + 1)/(x + 1) = xR1$

Arithmetic mod $x^2 + x + 1$

+	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

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 x