MATH 314 - Class Notes

9/29/2016

Scribe: Taylor Hamilton

Summary: Today's class covered why 3-pass protocol isn't perfect and fields.
Notes:

Reasons why 3-pass protocol isn't perfect:

1. There are 3 times as many messages being sent.
2. It is vulnerable to the "intruder in the middle" attack.

Fields
A Ring is a set of elements you can add/subtract/multiply.

A Field is a ring where you can divide by every non-zero element.

Examples:

- Ring of integers modulo a prime number
- Real numbers
- Rational numbers (fractions)

Non-Examples:

- Integers (can't do division)
- n x n matrices (not all matrices are invertible)
- Polynomials with integer coefficients
- Rings of integers modulo a composite integer n

A Finite Field is a field with a finite many elements.
Example:p=3 the field modulo 3 has 3 elements $\{0, 1, 2\}$

Theorem: for any integer n there is at most one field with n elements.

- Write $\mathbb{F}_n$ for the field with n elements if it exists
- $\mathbb{F}_3$ is the ring of integers modulo 3
- $\mathbb{F}_p$ is the ring of integers modulo p if p is a prime number
- Write $\mathbb{F}_p[x]$ when doing math on polynomials with coefficients in a finite field

Example: $\mathbb{F}_2[x]$
Let $f(x) = x^3 + x^2 + 1 = 1x^3 + 1x^2 + 0x + 1$
Let $g(x) = x + 1 = 1x + 1$

Compute $f(x) + g(x)$:

$$\begin{array}{r} x^3 + x^2 + 0x + 1 \\ + \qquad\qquad 1x + 1 \\ \hline x^3 + x^2 + x + 0 \end{array}$$

$f(x) + g(x) = x^3 + x^2 + x$

Compute $f(x)g(x)$:
FOIL $(x^3 + x^2 + 1)(x + 1)$
$= (x^4 + x^3 + x) + (x^3 + x^2 + 1)$
$= x^4 + x^2 + x + 1$

Weird fact in $\mathbb{F}_2[x]$ *addition and subtraction are the same thing*