Syllabus: Introduction to Algebraic Information Theory for Quantitative Finance

August 30, 2025

Timothy Tarter
James Madison University
Department of Mathematics

Overview

The goal of this class is to cover topics in Abstract Algebra I & II, Number Theory, Algebraic Cryptography, and Information Theory. It will be a seven-week course starting on June 30 and ending August 14. Lectures will be held every Monday evening from 6:30-10:00 PM over Microsoft teams. There will be a weekly homework, a weekly definition quiz, and occasional programming assignments. Additionally, there will be a cumulative final at the end of the course.

Reference Texts

This course uses the following textbooks as a guide for lectures:

1. Herstein, Abstract Algebra 3rd Edition
2. Matsuura, A Friendly Introduction to Abstract Algebra 2nd Edition
3. Howie, Fields and Galois Theory
4. Trappe and Washington, Introduction to Cryptography and Coding Theory Second Edition
5. Lidl and Pilz, Applied Abstract Algebra Second Edition
6. Silverman, Rational Points on Elliptic Curves

Grades

This class is an explicit prerequisite for individuals in the Madison Institute for Mathematical Finance to work under me as a researcher; thus, the class is of a pass-fail nature. A "passing grade" is 85%. I.e., 85% is the minimum grade I feel comfortable saying "this person knows xyz

material because I taught it to them." I am a fairly lenient grader - especially on homeworks, so grades will not be adjusted or rounded at the end of the course. The grade split will be as follows:

- 10% Homework 1
- 2% Definition Quiz 1
- 10% Homework 2
- 2% Definition Quiz 2
- 10% Homework 3
- 2% Definition Quiz 3
- 10% Homework 4
- 2% Definition Quiz 4
- 10% Homework 5
- 2% Definition Quiz 5
- 10% Programming assignment 1
- 10% Programming assignment 2
- 20% Cumulative final

Programming Assignments

1. Elliptic Curve Integer Factoring Algorithm (Lenstra)
2. Reed-Solomon Code Encryption / Decryption
3. Bonus: Shamir Secret Sharing

All assignments to be completed in Python.

Course Topics:

Anything with * next to it will be formally proven in classes.

Week 1: An Introduction to Abstract Algebra

Intro to group theory, homomorphisms, quotient groups, homomorphism theorems, commutative diagrams, Fundamental Theorem of Finite Abelian Groups.

Week 2: Finishing Up Finite Group Theory + An Introduction to Rings

Cyclic groups and order, Lagrange's Theorem, Cauchy's Theorem, Cayley theorems, Sylow Theorems, Bezout's Identity, Euclidean Algorithm (and Extended), Modular Inverses, CRT, FLT, Euler's φ function, RSA encryption as an example, intro to rings, $ID \to PID \to ED \to$ Field, Ideals.

Week 3: Polynomial Rings

Cover polynomial Rings, Gauss' Lemma, Eisenstein Criterion, field extensions, field of quotients, vector spaces and modules, field extensions are vector spaces, algebraic extensions, canoncial extensions of fields and roots of polynomials, splitting fields, finite fields.

Week 4: Galois Theory

Galois groups, K-Automorphisms, Galois Correspondence, $E \subseteq \Phi(\Gamma(E))$, $H \subseteq \Gamma(\Phi(H))$, root extension theorem.

Week 5: Galois Theory Continued

Normal extensions and normal closures, seperable extensions, perfect fields, all finite fields are perfect, fundamental theorem of Galois Theory, Hilbert's basis theorem, solvable groups, all finite abelian groups are solvable, S_3, S_4 are solvable, A_n $(n \geq 5)$ is simple, S_5 is not solvable, tying polynomial solutions to Galois groups, general quintics have no solution.

Week 6: Elliptic Curve Cryptography

Elliptic curve week! Start on elliptic curves as an example of monic polynomials in cryptography, show pointwise addition, general group structure, and cover the elGamal signature and Identity Based Encryption structure.

Week 7: Cryptographic Algorithm Survey

Cover LFSR Sequences, DES and AES, then move to Lagrange Interpolation, secret splitting ciphers, basic linear codes, zero knowledge proofs, review probability theory, Shannon Entropy, perfect secrecy, and cover Huffman codes. End with lattice methods as an attack on RSA and NTRU ciphers (and respective attacks), then error correcting codes.