

Course Goals: Math 441, Abstract Algebra I

Catalog description: This introductory course in abstract algebra is focused mainly on number theory, with an introduction to the concepts of groups, rings, and fields. Number theoretic concepts include divisibility (such as Bezout's identity, the fundamental theorem), congruences, number-theoretic functions, Euler's Theorem, linear Diophantine equations, Quadratic Reciprocity, and applications to cryptography.

Within each topic, student will demonstrate the following:

I. Divisibility Theory

- Prove the division algorithm
- Apply the division algorithm
- Prove the Euclidean algorithm
- Apply the Euclidean algorithm
- Prove Bezout's identity $ax + by = \gcd(a, b)$ and common corollaries.
- Apply Bezout's identity.
- Solve linear Diophantine equations of the form $ax + by = c$; including determination of conditions for solvability as well as a complete solution set, along with justification.

II. Primes

- Prove the Fundamental Theorem of Arithmetic
- Apply the Fundamental Theorem of Arithmetic
- State and apply Dirichlet's theorem on the distribution of primes
- Demonstrate knowledge of the statement of Goldbach's conjecture

III. Congruence Theory

- Prove and apply the basic properties of congruences
- Solve linear congruences completely
- Solve a system of congruences, for some sampling of a system
- Prove Fermat's Little Theorem
- Apply Fermat's Little Theorem
- Prove Euler's Generalization of Fermat's Little Theorem
- Apply Euler's Generalization of Fermat's Little Theorem
- Prove Wilson's Theorem
- Apply Wilson's Theorem
- Encrypt and decrypt a message using the method of RSA codes, including authentication.

IV. Multiplicative Functions

- Demonstrate familiarity with the definition and calculation of the Euler Phi function ϕ
- Demonstrate familiarity with the definitions and calculation of the τ and σ .
- Prove that a specified number theoretic function is multiplicative
- Solve computational problems using properties of functions such as ϕ , τ and σ .

V. Fermat's Last Theorem

- Demonstrate knowledge of some of the history of Fermat's Last Theorem, it's place in the history of mathematics

VI. Primitive Roots

- Calculate the order of a number $(\text{mod } n)$
- State the definition of primitive root.
- State theorem characterizing which numbers have primitive roots.
- Determine a primitive root for a number of the form $n = 2, 4, p^k$, and $2p^k$, where p is an odd prime and $k \geq 1$ and determine how many distinct primitive roots exist for the number in question.

VII. Introduction to groups

- Define group, order of a group and order of an element of a group.
- Define the groups $(Z_n, + \text{mod } n)$ and $(U_n, + \text{mod } n)$.
- Determine order of the groups $(Z_n, + \text{mod } n)$ and $(U_n, + \text{mod } n)$, and the order of specified elements of such groups.
- Determine generators for $(Z_n, + \text{mod } n)$ and $(U_n, + \text{mod } n)$, in the case that the group is cyclic.

VIII. Computation

- Explore number theoretic calculations on a hand-held calculator and demonstrate knowledge of the limits and reliability of this tool.
- Use a CAS, such as Mathematica, to explore a number theory problems that exceed the capacity of a hand-held calculator, such as RSA encryption examples.

IX. Quadratic Reciprocity

- Demonstrate knowledge of and be able to prove the basic properties of the Legendre symbol
- Demonstrate knowledge of the statement of and be able to apply the law of quadratic reciprocity
- Demonstrate knowledge of and be able to prove which primes have -1 as a quadratic residue