MATH 605: Number Theory
Credits: 3
Term(s) to be offered: Spring
Prerequisite(s): MATH 566; MATH 519 and 567, or concurrent registration.

Instructor: Chosen from among mathematics faculty.

Mode of Delivery: Classroom lectures by instructor.

Methods of Evaluation: Grades will be based approximately as follows: homework 60%, oral presentations 15%, and written final projects 25%. Grade distribution will be approximately 70% A, 25% B, 5% C.

Version A) Algebraic Number Theory

Course description: Algebraic number theory, with an emphasis on number fields, including factorization in rings of integers of number fields and ramification in extensions of number fields. Applications to reciprocity laws and cryptography. Exposure to active research problems on class groups, ramification, and Galois theory.

Text(s): Sample texts include
Algebraic Number Fields (Janusz)
Algebraic Number Theory (Lang)
Classical Theory of Algebraic Numbers (Ribenboim)

Course objectives: After successfully completing this course, the student will be able to:

- Prove results about algebraic number fields and their extensions.
- Compute invariants in algebraic number theory, such as discriminants and automorphism groups.
- Understand the theory of ideal factorization and the theory of abelian extensions of number fields.
- Start graduate research in number theory.

Sample weekly schedule: (may vary somewhat depending on instructor and choice of text)
Week 1: Introduction, finite fields.
Week 2: Quadratic fields, quadratic reciprocity.
Week 3: Cyclotomic fields, norm and trace maps.
Week 4: Number fields and their extensions, integral basis, the discriminant.
Week 5: Ramification, Kummer's theorem, residue field extension.
Week 6: Unique factorization, ideal class group.
Week 7: Norms of ideals, Minkowski theory, applications to lattice-based cryptography.
Week 8: Kummer's proof of Fermat's Last Theorem for regular primes.
Week 9: Localizations, discrete valuation rings.
Week 10: Frobenius automorphism, Artin map.
Week 11: Automorphisms of algebraic number fields, Galois theory.
Week 12: Abelian extensions of the rationals, Kronecker-Weber theorem.
Week 13: Noether's theorem, Hilbert's irreducibility theorem.
Week 14: Inverse Galois theory.

Weeks 15 and 16: Oral presentations.

Version B) Arithmetic Geometry

Course description: Number theory from the perspective of arithmetic geometry, with an emphasis on arithmetic function fields and zeta functions. Applications to Diophantine equations and cryptography. Exposure to active research problems on function field extensions and L-functions.

Text(s): Sample texts include
A Classical introduction to Modern Number Theory (Ireland/Rosen)
An Invitation to Arithmetic Geometry (Lorenzini)

Course objectives: After successfully completing this course, the student will be able to:

- Prove results about Diophantine equations and zeta functions.
- Compute invariants in arithmetic geometry, such as Gauss sums or Euler products.
- Understand the theory of arithmetic function fields and L-functions.
- Start graduate research in number theory.

Sample weekly schedule: (may vary somewhat depending on instructor and choice of text)
Week 1: Introduction, global fields.
Week 2: Quadratic fields, quadratic Gauss sums.
Week 3: Multiplicative characters, Gauss and Jacobi sums.
Week 4: Arithmetic function fields, Diophantine equations.
Week 5: Function fields and their extensions, genus, ramification.
Week 6: Diophantine approximation, Roth's theorem.
Week 7: Pell's equation, units in quadratic fields.
Week 8: Zeta functions and L-functions.
Week 9: Analytic continuation, Euler product, functional equation.
Week 10: Riemann hypothesis, prime number theorem, applications to public-key cryptography.
Week 11: Dedekind zeta functions, Chebotarev density theorem.
Week 12: Dirichlet L-functions, Dirichlet's theorem on arithmetic progressions.
Week 13: Zeta functions of curves over finite fields, Hasse-Weil bound.
Week 14: Weil conjectures.
Weeks 15 and 16: Oral presentations.

Version C) Elliptic curves

Course description: Elliptic curves, as the fundamental example of a group variety, including points on elliptic curves defined over the complex numbers, number fields and finite fields. Applications to Hilbert's 10^{th} problem and elliptic curve cryptography. Exposure to active research problems on Galois representations and modular curves.

Text(s): Sample texts include

The Arithmetic of Elliptic Curves (Silverman)
Elliptic Curves (Milne)

Course objectives: After successfully completing this course, the student will be able to:

- Prove results about points on elliptic curves and Galois representations.
- Compute invariants of elliptic curves, such as the j-invariant and modular forms.
- Understand the connection between elliptic curves and Fermat's Last Theorem and the theory of modular curves.
- Start graduate research in number theory.

Sample weekly schedule: (may vary somewhat depending on instructor and choice of text)

Week 1: Introduction, cubic equations, elliptic curves, the group law.
Week 2: Torsion points, reduction of elliptic curves, Nagell-Lutz theorem.
Week 3: Complex tori, Weierstrass model, j-invariant, elliptic functions.
Week 4: Endomorphisms, automorphisms, isogenies, pairings.
Week 5: Heights, Mordell's Theorem.
Week 6: Zeta functions of elliptic curves, Hecke L-functions.
Week 7: Rank, Birch and Swingerton-Dyer Conjecture, applications to Hilbert's 10^{th} problem.
Week 8: Galois representations, Tate module.
Week 9: Complex multiplication, application to abelian extensions of quadratic fields.
Week 10: Supersingular elliptic curves, application to cryptography.
Week 11: Modular forms, conductor, level.
Week 12: Modular curves, quotient of upper half plane by congruence subgroups.
Weeks 13 and 14: Fermat's Last Theorem or Complex abelian varieties.
Weeks 15 and 16: Oral presentations.