University of Maine – Department of Mathematics & Statistics
MAT 500 – Introduction to Modern Number Theory
Spring 2024

Instructor: Jack Buttcane, jack.buttcane@maine.edu

Lecture: MWF 9:00-9:50am in Neville Hall 421

Credits: 3

Prerequisites: Undergraduate or graduate real or complex analysis

Depending on the background of the students, we will start by covering some topics from the undergraduate course and proceed to more advanced topics in elementary, analytic, geometric and/or algebraic number theory:

- Analytic number theory uses the methods of analysis; a classical theorem is that the count of prime numbers less than x is (roughly) $x/\log x$ and, for any integer q, these are (almost) evenly divided into equivalence classes $a \pmod{q}$ with a coprime to q. Some other flavors: A typical question in additive number theory is: can every number be written as a sum of three cubes? (Not quite.) A typical question in multiplicative number theory is: how many divisors does a typical number have? (n has roughly $\log n$ divisors, on average.)

- Algebraic number theory uses the methods of (abstract) algebra; a fairly recent theorem is that for n an integer greater than 2, $x^n + y^n = z^n$ has only the trivial solution $x = y = z = 0$ in integers. A common object of study is a number field, i.e. a finite field extension of $\mathbb{Q}$; e.g. ., in the number field $\mathbb{Q}[i]$ where $i^2 = -1$, which elements should be considered "integers"? Which of these should be considered "prime"?

- Geometric number theory uses methods of geometry; a classical theorem is that any convex set in $\mathbb{R}^2$ that is symmetric about the origin and has area greater than 4 must contain a point of $\mathbb{Z}^2$ other than the origin. Related areas are Diophantine geometry and Diophantine approximation; a classical theorem is that for any irrational number α, there are infinitely many rational numbers p/q such that $|\alpha - p/q| < 1/q^2$.

- Elementary number theory excludes the use of complex analysis (which often makes the proofs much less elementary). One notable entry in this category is sieve theory; an ancient result is the Sieve of Eratosthenes, which is an efficient way of finding (small) prime numbers.

- Applied number theory typically (but not exclusively) refers to encryption; i.e. how do I send someone a message that only they can read? Computational number theory asks for efficient methods of computing solutions to number-theoretic problems; e.g. how do I find a large (random) prime number? or how can I quickly find integer solutions to this algebraic equation (if they exist)?

My particular area is automorphic forms which involves applying analytic and algebraic methods (I'm more on the analysis side) to study a nice basis of the L^2 space over $SL(n,\mathbb{Z})\backslash GL(n,\mathbb{R})$, and this has applications to many areas of number theory.