10th Annual Upstate Number Theory Conference

Union College, Schenectady, NY

October 23-24, 2021

Plenary Speaker Abstracts

Shabnam Akhtari (University of Oregon)

How to count integral (cubic and quartic) binary forms

To study interesting arithmetic properties of integral binary forms, we often need a way to order them. I will discuss some natural ways to order binary forms $F(x, y)$ with integer coefficients, especially those of degree 3 and 4. I will show some of my recent work as examples of the importance of understanding the invariant theory of integral binary forms in order to count these important arithmetic objects.

Renee Bell (University of Pennsylvania)

Monodromy of tamely ramified covers of the projective line

The étale fundamental group π_1^{et} in algebraic geometry formalizes an analogy between Galois theory and topology, extending our intuition to spaces in which loops, as defined traditionally, do not yield meaningful information. For a curve X over an algebraically closed field of characteristic 0, finite quotients of $\pi_1^{et}(X)$ can be described solely in topological terms, but in characteristic p, dramatic differences and new phenomena have inspired many conjectures. Let k be an algebraically closed field of characteristic p and let X be the projective line over k with three points removed. In joint work with Booher, Chen, and Liu, we show that for each prime $p \geq 5$, there are families of tamely ramified covers with monodromy the symmetric group S_n or alternating group A_n for infinitely many n, producing these covers from moduli spaces of elliptic curves.

Andrew Sutherland (mit)

ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$

I will discuss some recent progress on Mazur's "Program B" that is joint work with Jeremy Rouse and David Zureick-Brown. We obtain a provisional classification of the possible images of ℓ-adic Galois representations associated to elliptic curves over that is provably complete barring the existence of unexpected rational points on modular curves associated to the normalizers of non-split Cartan subgroups and two genus 9 modular curves of level 49. As an application, we obtain an efficient algorithm to rigorously determine the ℓ-adic image of

Galois of an elliptic curve over at all primes ℓ. We have applied this algorithm to all of the elliptic curves $E/$ in the L-functions and modular forms database (LMFDB), including all elliptic curves of conductor up to 500,000.

Christelle Vincent (University of Vermont)

Post-quantum cryptography: What is it and why?

You might have heard of quantum cryptography and post-quantum cryptography, and wondered if those are the same or different (they are different!). This might have prompted you to ask the deeper question of what quantum physics has to do with cryptography, or even revealed to yourself that you aren't really sure how cryptography works at all! This talk is meant to address all of this in an informal and fun atmosphere. More specifically, I will introduce the basics of modern public-key cryptography, discuss how the possibility of large quantum computers affects the security of current cryptographic algorithms, and finally convince you that mathematicians are needed to design the algorithms of the future.

Jared Weinstein (Boston University)

Higher modularity of elliptic curves

This is joint work with Adam Logan. Elliptic curves E over the rational numbers are known to be modular, in the sense that there is a uniformization of E by a modular curve. When E is an elliptic curve over a function field, one gets an analogous notion of modularity, where E is uniformized by a Drinfeld modular curve. But one can also formulate for each natural number r a notion of "r-modularity", predicted by Tate's Conjecture: the self-product E^r should admit a correspondence to a space of "r-legged shtukas". We show that a few examples of E, including the Legendre family, are 2-modular.