NUMBER THEORY AND ARITHMETIC GEOMETRY SESSION

Ehud de Shalit (Hebrew University)

Difference equations and algebraic independence over elliptic function fields

A general theme that emerged in various works in recent years says that if two complex power series satisfy linear homogenous difference (or differential) equations with polynomial coefficients, with respect to two difference (differential) operators that are sufficiently independent, then either one of the power series is a rational function, or the two power series are algebraically independent over $\mathbb{C}(x)$. We prove an analogous theorem over fields of elliptic functions. Two new issues that arise are questions of periodicity of solutions, and the connection to Atiyah's theory of vector bundles over elliptic curves.

Mark Shusterman (Harvard University and Weizmann Institute of Science)
2022 Levitzky prize winner

The geometric Boston-Markin conjecture

Given a finite simple group G, we realize it as a Galois group with a single ramified prime over $\mathbb{F}_p(x)$ for some prime number p. This involves a study of the connected components of generalized Hurwitz spaces.

Ariel Weiss (Ben-Gurion University)

The Lang-Trotter Conjecture and its generalisations

Let $E/\mathbb{Q}$ be an elliptic curve and, for each prime p, let $a_p = p+1-|E(\mathbb{F}_p)|$. Alternatively, let $f = \sum_n a_n q^n$ be a modular eigenform with integer Hecke eigenvalues. What integers a can occur as one of the a_p's? What integers a can occur as one of the a_p's for infinitely many primes p? For a given integer a, what can we say about the asymptotics of the sets $\{p \leq x : a_p = a\}$ as $x \to \infty$?

In 1976, Serge Lang and Hale Trotter formulated a precise conjecture that proposes an answer to all of these questions, in the case of elliptic curves. Their heuristics can be generalised to formulate similar conjectures for modular forms as well. However, all these conjectures are wide open!

The goal of this talk is to give an introduction to the Lang-Trotter conjecture, as well as its connection to other famous problems. If time permits, I will discuss recent work with Arvind Kumar and Moni Kumari, in which we give upper bounds on the sizes of the sets $\{p \leq x : a_p = a\}$ when the a_p are the Hecke eigenvalues of a genus 2 Siegel modular form.

David Corwin (Ben-Gurion University)

Selmer groups and rational points on curves

Faltings' theorem states that an algebraic curve of genus 2 or greater has finitely many rational points over any number field. The question of bounding the number of or finding the rational points is an area of ongoing research. The non-abelian Chabauty's method of Minhyong Kim relates this to subgroups of Galois cohomology known as Bloch-Kato Selmer groups.

We first define these groups and state part of the Bloch-Kato conjectures bounding their ranks. We then describe a bound joint with A. Betts and M. Leonhardt on the number of rational points on a general higher genus curve, conditional on these conjectures. We mention briefly how one may use Iwasawa theory to prove cases of these conjectures. Finally, as time allows, we discuss work, partly joint with I. Dan-Cohen, on finding explicit p-adic equations for the rational points.