Number Theory
Théorie des nombres
(Org: **Alina C. Cojocaru** (Illinois-Chicago) and/et **Damien Roy** (Ottawa))

SHABNAM AKHTARI, Queen's
Quartic Thue Equations

Applying the theory of linear forms in logarithms, we will give upper bounds upon the number of integral solutions to binary quartic Thue equations. We will treat a certain family of quartic binary forms using a classical theorem of Thue based on Padé approximation to binomial functions. We shall also discuss the relation between the number of integral solutions to quartic Thue equations and integral points on elliptic curves.

YURI BILU, Université Bordeaux 1
Uniformity in Galois Representations

We prove that there exists an integer p_0 such that for any non-CM elliptic curve E over $\mathbb{Q}$ and any prime $p > p_0$ the image of the representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ induced by the Galois action on the p-division points of E is not contained in the normalizer of a split Cartan subgroup. This gives a partial answer to an old question of Serre.

NILS BRUIN, Simon Fraser University, Burnaby, BC
Fake Selmer sets of curves

We consider the problem of determining if a curve has any rational points. A first step in deciding this is to see if the curve has points everywhere locally. This is a necessary, but not sufficient condition for having rational points.

A refined criterion is obtained by considering an unramified Galois cover of the curve. If the curve has a rational point, then one of finitely many twists of the cover has a rational point as well, and hence there must be a twist that has point everywhere locally. This method is referred to as a *finite descent* on the curve, and the collection of everywhere locally solvable covers is called a *Selmer set* of the curve.

We present a method that computes an object that is closely related to the Selmer set, but is much easier to compute. We also present some statistics on the effectiveness of this descent obstruction compared to local obstructions.

BRYDEN CAIS, McGill

STEPHEN CHOI, Simon Fraser University
An extension to the Brun–Titchmarsh theorem

The Siegel–Walfisz theorem states that for any $B > 0$, we have $\sum_{p \le x, p \equiv d \pmod v} 1 \sim x/\varphi(v)\log(x)$ for $v \le \log^B(x)$ and $(v, d) = 1$. This only gives an asymptotic formula for the number of primes in an arithmetic progression for quite a small modulus v compared to x. However, if we are concerned only with an upper bound, the Brun–Titchmarsh theorem says that for any $1 \le v \le x$, we have $\sum_{p \le x, p \equiv d \pmod v} 1 \ll x/\varphi(v)\log(x/v)$. In this talk, we will discuss an extension to the Brun–Titchmarsh theorem that concerns the number of integers with exactly s distinct prime factors in an arithmetic progression.

This is joint work with Kai Man Tsang and Tsz Ho Chan.

ALINA C. COJOCARU, University of Illinois at Chicago
Serre curves in one parameter families

In 1972, Serre proved that the Galois groups of the n-division fields of a non-CM elliptic curve over Q are as large as possible, provided that n is sufficiently large. I will discuss what "sufficiently large" means when one looks at a one-parameter family of elliptic curves.

This is joint work with David Grant and Nathan Jones.

CHANTAL DAVID, Concordia University
Almost prime orders of elliptic curves over finite fields

Let E be an elliptic curve over the rationals. A conjecture of Neal Koblitz predicts an exact asymptotic for the number of primes p such that the order of E over the finite field with p element is prime. This conjecture is still open. Using sieve techniques, one can find a lot of primes p such that the order $p+1-a_P(E)$ is almost prime. The best result that one may hope to achieve by sieve techniques was obtained by Iwaniec and Jimenez Urroz for complex multiplication curves using Chen's sieve. They showed that there are infinitely many primes p such that $p+1-a_p(E) = P_2$, where $n = P_k$ means that the integer n has at most k prime factors. For elliptic curves without complex multiplication, it is not known how to apply the switching principle of Chen's sieve to get such a result.

For curves without complex multiplication, we show that there are many primes p such that $p+1-a_p(E) = P_8$ with an explicit lower bound (in terms of the constant $C(E)$ of Koblitz's conjecture), using Greaves' sieve and under the GRH. This improves previous work of Steuding and Weng. One can also show that there are many primes such that $p+1-a_p(E)$ has at most 6 *distinct* prime factors, but still cannot improve the number of (not necessarily distinct) primes from 8 to 6. This surprising result is related to the difficulty of sieving square-free numbers in the sequence $p+1-a_p(E)$.

This is joint work with Jie Wu (CNRS, Institut Elie-Cartan, Nancy).

ERNST KANI, Queen's University, Kingston, Ontario
Curves of genus 2 and a Conjecture of Gauss

The purpose of this talk is to explain how an (extended) conjecture of Gauss plays a role in determining pairs of elliptic curves (E, E') which have the property that there is a curve of genus 2 on the product surface $E \times E'$.

STEPHEN KUDLA, University of Toronto, 40 St. George St., Toronto, ON, M5S 2E4
Arithmetic cycles for unitary groups

In this talk, I will discuss some recent work with Rapoport on arithmetic cycles for Shimura varieties associated to $U(n-1,1)$. In particular, we establish a relation between the arithmetic degrees of certain 0-cycles and the nonsingular, nondegenerate Fourier coefficients of the derivatives of certain incoherent Eisenstein series on $U(n,n)$. If time permits, I plan to discuss various low dimensional examples and some explicit formulas for local height contributions.

RAM MURTY, Queen's University, Kingston, Ontario
Special values of L-series and transcendental numbers

We discuss some recent progress in transcendental number theory. More precisely, we will examine special values of certain L-series and determine when these are transcendental numbers. In particular, we study class group L-functions attached to imaginary quadratic fields.

This is a report of joint work with V. Kumar Murty as well as Sanoli Gun and Purusottam Rath.

MICHAEL RUBINSTEIN, University of Waterloo, 200 University Ave. W, Waterloo, ON, N2L 3G1
Computing lower terms for the moments of the zeta function

A 100-year-old problem asks to determine the moments of the Riemann zeta function on $\Re s = 1/2$. The second and fourth moments are well understood, but little has been proven about the higher moments. These moments are needed to understand the distribution of the zeta function and its extreme behaviour.

In recent years, a detailed conjectural picture has emerged concerning the full asymptotics of the moments of the zeta function. I will describe these developments and describe methods to compute the coefficients of the polynomials that appear in these asymptotics.

KENNETH WILLIAMS, Carleton University, Ottawa
The (p, k)-calculus for quadratic forms

A simple method will be described for determining the number of representations of a positive integer n by a quadratic form $a_1x_1^2 + \cdots + a_{2k}x_{2k}^2$, where k is a positive integer and $a_1, \ldots, a_{2k}$ are positive integers whose prime factors belong to $\{2, 3\}$.

This is joint work with A. Alaca and S. Alaca.