Explicit Number Theory

Valparaíso, January 2019

Titles and abstracts of the talks

The difficulty of proving effective results for norm form equations

Shabnam AKHTARI (University of Oregon, and Max-Planck Institute, Bonn)

Abstract Let $\omega_1, \ldots, \omega_n$ be algebraic numbers that are linearly independent over the rationals, and let $k = \mathbb{Q}(\omega_1, \ldots, \omega_n)$. We define a homogeneous polynomial in n variables $x_1, \ldots, x_n$ by

$$N(\mathbf{x}) = \mathrm{Norm}_{k/\mathbb{Q}}(x_1\omega_1 + \ldots + x_n\omega_n).$$

We are interested in the points in $\mathbb{Z}^n$ that satisfy the equation $N(\mathbf{x}) = b$, for a fixed non-zero $b \in \mathbb{Q}$. In his breakthrough work on norm form equations, Wolfgang Schmidt used his celebrated Subspace Theorem to prove that norm form equations have finitely many families of solutions. Schmidt also obtained some bounds on the number of families of integer solutions to norm form equations. We are interested in finding effective bounds for the height of the representatives of integral solutions of norm form equations. I will describe some recent work, joint with Jeffrey Vaaler, for a particular type of norm equation. Then I will try to explain the difficulty of obtaining such results for general norm form equations.

Sum of two S-units via Frey-Hellegouarch curves

Nicolas BILLEREY (Université Clermont-Auvergne)

Abstract In this talk we shall describe a method for explicitly finding all perfect powers that can be expressed as the sum of two integral S-units, where S is a fixed finite set of primes. Our approach, which is based on the modularity of some attached Galois representations, local arguments and heavy computations on Thue and Thue-Mahler equations, allows us to explicitly solve the problem for some small sets of primes such as $S = \{2, 3\}$ and $S = \{3, 5, 7\}$. This is a joint work with Michael A. Bennett.

Fields of algebraic numbers with non-uniformly bounded local degrees and their Galois groups.

Sara CHECCOLI (Institut Fourier, Université Grenoble Alpes)

Abstract It is known that, if K is a number field and L/K is an infinite Galois extension, then the local degrees of L are uniformly bounded at all rational primes if and only if the group Gal(L/K) has finite exponent.

Also motivated by some problems concerning the Bogomolov property (on the existence of a lower bound for the elements of non-zero height in a field), one can ask whether the simple non-uniform boundedness of the local degrees of L is still equivalent to some (weaker) group theoretical property of Gal(L/K).

We will show that this is not the case in general, by exhibiting several groups that admit two different realisations over a given number field, one with bounded local degrees at a given set of primes and one with infinite local degrees at the same primes.

Computing L-functions of Dirichlet characters at negative integers

Henri COHEN (Université de Bordeaux, LFANT, INRIA, IMB)

Abstract We survey a number of different methods for computing $L(\chi, 1-r)$, where χ is a Dirichlet character, in particular quadratic. In particular this has applications to the computation of lambda invariants of quadratic fields. The main conclusion is that when r is not too large (for instance $r \leq 100$) the best method comes from the use of Eisenstein series of half-integral weight, while when r is large the best method is the use of the complete functional equation, unless the conductor of χ is really large, in which case the previous method again prevails.

On particular values of certain special functions

Milton ESPINOZA (Universidad de Valparaíso)

Abstract A standard approach to the study of particular values of special functions involves seeking functional equations arisen from suitable groups of substitutions. For example, for the Riemann zeta function $\zeta(s)$ and the substitution $s \mapsto 1 - s$, we have the functional equation

$$\zeta(s) = 2^s \pi^{s-1} \sin\Big(\frac{\pi s}{2}\Big)\Gamma(1-s)\zeta(1-s).$$

Some problems in number theory encourage us to deal with special functions of several variables, for which it would be desirable to have any handy functional equation, hopefully, as good as the above.

In this talk, we will introduce a novel functional equation for a special function of several variables that goes back to Barnes, and we will illustrate its scope by means of examples relating it to different kinds of functions: modular forms, Dirichlet L-functions, and conditionally convergent series.

A case of the Rodriguez-Villegas conjecture

Eduardo FRIEDMAN (Universidad de Chile)

Abstract Let L be a number field and let E be any subgroup of the units $\mathcal{O}_L^*$ of L. If $\mathrm{rank}_{\mathbb{Z}}(E) = 1$, Lehmer's conjecture predicts that the height of any non-torsion element of E is bounded below by a positive constant independent of L. If $\mathrm{rank}_{\mathbb{Z}}(E) = \mathrm{rank}_{\mathbb{Z}}(\mathcal{O}_L^*)$, Zimmert proved a lower bound on the regulator of E which grows exponentially with $[L : \mathbb{Q}]$.

Fernando Rodriguez Villegas made a conjecture in 2002 that "interpolates" between these two extremes of rank. We will describe this conjecture and mention a recently proved high-rank case of it. This is joint work with Ted Chinburg and James Sundstrom.

Ranks of elliptic curves and arithmetic progressions of rational points

Natalia GARCIA-FRITZ (Pontificia Universidad Catolica de Chile)

Abstract In 1980, Mohanty conjectured that a sequence of rational points on a Mordell elliptic curve whose x-coordinates are in arithmetic progression cannot have more than four terms. Based on theoretical and numerical evidence, Bremner conjectured that rational points of elliptic curves with x-coordinates in arithmetic progression should tend to be independent in the group of rational points. Thus, it is expected that the maximal length of a sequence of this type on an elliptic curve E should be bounded in terms of the rank of E. In joint work with Hector Pasten, we prove that the maximal length of an arithmetic progression on an elliptic curve can be bounded in terms of its rank and its j-invariant only. As a consequence, we prove Bremner's conjecture for families of twists of elliptic curves, and in particular, we deduce that Honda's conjecture implies a general version of Mohanty's conjecture. Furthermore, we unconditionally prove Mohanty's conjecture for large families of Mordell elliptic curves. Our result also allows us to unconditionally answer questions on arithmetic statistics related to long x-arithmetic progressions, such as finiteness of the average length on quadratic twist families.

Torsion bounds for abelian varieties

Éric GAUDRON (University Clermont Auvergne, France)

Abstract Let (A, L) be a polarized abelian variety over a number field K. A point $P \in A(K)$ is called a torsion point if there exists a positive integer n such that $nP = 0$. The group of torsion points of $A(K)$ is finite. In this talk we shall present several bounds of its cardinality in terms of the degree of K, the dimension and Faltings height of A. This is joint work (in progress) with Gaël Rémond.

Explicit local Langlands correspondence

Guy HENNIART (Université Paris Sud Orsay)

Abstract Let F be a p-adic field. The Langlands correspondence for $G = \mathrm{GL}(n, F)$ relates irreducible representations of G to n-dimensional representations of the absolute Galois group of F. When $n = 1$, it is class field theory. We shall examine to which extent an explicit description of the case $n = 1$ for F and its finite extensions can lead to an explicit description in the general case.

Mock modular forms whose shadows are Eisenstein series

Sebastián HERRERO (Chalmers U. of Technology and U. of Gothenburg)

Abstract Mock modular forms can be defined as holomorphic parts of harmonic Maass forms, which are functions on the upper-half plane that transform like classical modular forms, are annihilated by the hyperbolic Laplace operator and have at most linear exponential growth at cups.

Examples of mock modular forms have been known for many decades, but their theory was only systematically developed after the work of Zwegers on 2002 on the modularity of Ramanujan's mock theta functions. Since then, these functions have attracted the attention of many mathematicians.

There is a straightforward way of attaching to each mock modular form F a holomorphic modular form f, its *shadow*. This is obtained by applying certain differential operator to the harmonic Maass form having F has holomorphic part. In many contexts, given a holomorphic modular form f, it is useful to find explicitly a mock modular form F whose shadow is f.

The purpose of this talk is to present a simple and explicit construction of mock modular forms whose shadows are Eisenstein series of arbitrary weight, level, and character. This is joint work with Anna von Pippich (TU Darmstadt).

A tubular approach to Baker's method

Samuel LE FOURN (Warwick University)

Abstract Baker's method is one of the most widely used tools to obtain bounds on integral solutions of diophantine equations (or integral points on curves). In this talk, I will explain how it can also be applied on varieties and how it behaves there, before giving a further *tubular* generalization, giving new finiteness results in higher dimension but also better quantitative estimates in the special case of curves.

Reduction type of plane quartic curves

Elisa LORENZO (Université Rennes)

Abstract Let $C : F = 0$ be a plane quartic curve (i.e., a non-hyperelliptic genus 3 curve) and p a prime dividing its discriminant. The reduction modulo p of the model $F = 0$ is then singular, but we may wonder what is the reduction type of the stable model of C. In this joint work with R. Lercier, Q. Liu and C. Ritzenthaler, we give a criterion in term of the valuations of the Dixmier-Ohno invariants of the plane quartic to determine when C has potentially good (hyperelliptic or not hyperelliptic) reduction or geometrically bad reduction. Moreover, in the potentially good reduction cases, we determine the special fiber.

X-coordinates of Pell equations in various sequences

Florian LUCA (University of the Witwatersrand / University of Ostrava)

Abstract Let $d > 1$ be a squarefree integer and (X_n, Y_n) be the nth solution of the Pell equation $X^2 - dY^2 = \pm 1$. Given your favourite set of positive integers U, one can ask what can we say about those d such that $X_n \in U$ for some n? Formulated in this way, the question has many solutions d since one can always pick $u \in U$ and write $u^2 \pm 1 = dv^2$ with integers d and v such that d is squarefree obtaining in this way that (u, v) is a solution of the Pell equation corresponding to d. What about if we ask that $X_n \in U$ for at least two different n's? Then the answer is very different. For example, if U is the set of squares, then it is a classical result of Ljunggren that the only such d is 1785 for which both X_1 and X_2 are squares. In my talk, I will survey recent results about this problem when U is the set of Fibonacci numbers, Tribonacci numbers, k-Generalized Fibonacci numbers, sums of two Fibonacci numbers, rep-digits (in base 10 or any integer base $b \geq 2$), and factorials. The proofs use linear forms in logarithms and computations. These results have been obtained in joint work with various colleagues such as J. J. Bravo, C. A. Gómez, A. Montejano, L. Szalay and A. Togbé and recent Ph.D. students M. Ddamulira, B. Faye and M. Sias.

Casimir bilinear pairings and some arithmetic applications

Guillermo MANTILLA-SOLER (Universidad de los Andes)

Abstract I this talk I will show that totally real number fields, with fundamental discriminant, are completely determined by their integral trace pairing. The main new ingredient used to obtain such a result is the so called *Casimir pairing*. This is joint work with my M.Sc student Carlos Rivera-Guaca.

Proofs by example

Benjamin MATSCHKE (Koç University)

Abstract We study the proof scheme in which a general statement can be proved by verifying it for a single example. This strategy can indeed work if the statement in question is an algebraic identity and the example is "generic". This talk addresses the problem of constructing a practical example, which is sufficiently generic, for which the statement can be verified efficiently, and which even allows for a numerical margin of error.

Our method is based on diophantine geometry, in particular an arithmetic Bézout theorem, an arithmetic Nullstellensatz, and an effective Liouville–Łojasiewicz type inequality. As an application we discuss theorems from plane geometry and how to prove them by example.

Explicit Bounds for Primes in Arithmetic Progression

Kevin O'BRYANT (City University of New York, Staten Island)

Abstract We provide explicit bounds on $\pi(x;q,a)$, the number primes that $a \mod q$ and less than x. For $q > 3$, these are the first asymptotically correct explicit bounds. In this talk, I will state some of the results and independently interesting lemmas, and indicate why these results have not appeared earlier. Joint work with Michael A. Bennett, Greg Martin, and Andrew Rechnitzer.

The density of genus 1 curves in $\mathbb{P}^1 \times \mathbb{P}^1$ over $\mathbb{Q}$ that have points everywhere locally

Jennifer PARK (Ohio State University)

Abstract Consider a random homogeneous polynomial over $\mathbb{Q}$ of degree d in $n+1$ variables (which defines a hypersurface V of degree d in $\mathbb{P}^n$), where "random" denotes choosing its coefficients with equal likelihood in the interval $[-H, H]$. We say that V is everywhere locally soluble if for all places $\nu \leq \infty$ of $\mathbb{Q}$, the set $V(\mathbb{Q}_\nu)$ is nonempty, and globally soluble if $V(\mathbb{Q}) \neq \emptyset$. Poonen and Voloch conjecture that when $d < n+1$, everywhere locally soluble implies

globally soluble, and that when $d > n + 1$, the proportion of globally soluble hypersurfaces is 0. Thus, the most interesting case is when $d = n+1$, where there is a discrepancy between local and global solubility. Bhargava, Cremona, and Fisher explicitly compute the proportion of everywhere locally soluble curves when $d = 3$ and $n = 2$. In this talk, we generalize the Poonen-Voloch heuristics to hypersurfaces in products of projective spaces, and explicitly compute the proportion of everywhere locally soluble $(2, 2)$-curves in $\mathbb{P}^1 \times \mathbb{P}^1$, and also discuss the methods for the computation of more complicated boundary cases.

Bivariate polynomial injections of rational points

Héctor PASTÉN (P. Universidad Católica de Santiago)

Abstract I will prove that there is an affine curve C over $\mathbb{Q}$ with a dense set of rational points, and a polynomial function f on $C \times C$ defined over $\mathbb{Q}$ with the property that f induces an injective function $C(\mathbb{Q}) \times C(\mathbb{Q}) \to \mathbb{Q}$ on rational points.

Integrality Properties in the Moduli Space of Elliptic Curves

Stefan SCHMID (University of Basel)

Abstract There are infinitely many j–invariants of non–CM elliptic curves that are algebraic units. Let us fix a j–invariant j_0 of an elliptic curve without CM. In this talk I show that there are only finitely many j–invariants j that are algebraic units and such that curves corresponding to j and j_0 are isogenous. Moreover, we can give explicit bounds on the number of such j.

Congruences satisfied by eta quotients

Nicolás SIROLLI (Universidad de Buenos Aires)

Abstract Given a weakly holomorphic modular form f of integral or half-integral weight with Fourier coefficients $a(n)$, by using the quadratic twist method Treneer proved that, for certain primes p, a positive proportion of the primes Q satisfy that $a(Q^3 n) \equiv 0 \bmod p$ for all n coprime to Q satisfying a quadratic condition mod$p$.

In this talk we describe an algorithm for finding such primes p and Q when f is an eta quotient. We illustrate our method with a few examples.

This is work in progress, joint with Nathan Ryan, Zachary Scherr and Stephanie Treneer.

The Macdonald identities and Jacobi forms of lattice index

Nils SKORUPPA (Siegen)

Abstract We propose a new and short proof for the Macdonald identities using only some easy facts from the theory of Jacobi forms of lattice index and classical root systems. (The needed basic features of these theories will be explained in the talk). We discuss applications and open questions related to the new proof, and we end the talk by deducing from the Macdonald identities, for 42 elliptic curves over the rationals and of rank 1 product identities for the (classical) Jacobi forms attached to elliptic curves by the theory of modular forms.