Explicit p-Adic Methods in Number Theory
Sage Days 71

Abstracts of Talks

Jennifer Balakrishnan
Title: Variations on Chabauty-Coleman II

Abstract: I will discuss the computation of some iterated Coleman integrals that play a role in Kim's nonabelian Chabauty method to find rational points on curves. In particular, I will give a few examples in the case where the rank of the Jacobian is equal to the genus of the curve where this has been used in joint work with Dogra and Mueller to explicitly find rational points.

Francesca Bianchi
Title: Computation of Hida families of ordinary cusp forms

Abstract: The first example of a p-adic family of modular forms goes back to Serre's construction of the p-adic Eisenstein series. At the end of the 1980s Hida then introduced the notion of a p-adic family of modular forms going through a cuspidal eigenform in the ordinary subspace of a given weight. This means that we look for a q-expansion such that the coefficients depend p-adically on a parameter k, in such a way that specialising the expansion at a certain k gives an eigenform of weight k. In the talk we will present an algorithm to compute Hida families through an eigenform of trivial character.

Xavier Caruso
Title: p-adic Floats

Abstract: Floating point arithmetic is by far the most common implementation of real numbers on computers. This is in complete opposition with the p-adic case for which all standard implementations rely on interval arithmetic. This talk aims at arguing for initiating – and then generalizing – the use of p-adic floating point arithmetic in computer algebra systems.

Raf Cluckers
Title: Recent developments and applications of uniform p-adic integration

Abstract: As a concrete variant of motivic integration, we will discuss uniform p-adic integration and constructive aspects of results involved. Uniformity is in the p-adic fields, and, for large primes p, in the fields $\mathbf{F}p((t))$. Using real-valued Haar measures on such fields, one can study integrals, Fourier transforms, etc. We follow a line of research that Jan Denef started in the eighties, with in particular the use of (effective) model theory to study various questions related to p-adic integration. A form of uniform p-adic quantifier elimination is used, which is algorithmic. Using the notion of definable functions, one builds constructively a class of complex-valued functions which one can integrate (w.r.t. some of the variables) without leaving the class. One can also take Fourier transforms in the class. Recent applications in the Langlands program are based on Transfer Principles for uniform p-adic integrals, which allow one to get results for $\mathbf{F}p((t))$ from results for $\mathbf{Q}p$, once p is large, and vice versa. These Transfer Principles are obtained via the study of general kinds of loci, some of them being zero loci. More recently, these loci are playing a role in the uniform study of p-adic wave front sets for (uniformly definable) p-adic distributions, a tool often used in real analysis. This talk contains various joint work with Gordon, Halupczok, Loeser, Raibaut, and some of it is still in progress. Although all the definitions and results are algorithmic, almost nothing has been implemented yet, and questions about optimal complexity are far from being understood, although some lower bounds are known, coming from lower bounds for Presburger arithmetic.

Edgar Costa
Title: Zeta functions of quartic K3 surfaces over F_3

Abstract: With the goal of doing a census of the Hasse–Weil zeta functions of quartic K3 surfaces over **F**3, we overview the problem of computing the zeta function of a generic K3 surface over **F**3 using *p*-adic methods.

Alyson Deines
Title: Sage Number Theory and Development

Abstract: This talk will have three parts. In the first, I will discuss what number theoretic constructs are implemented in Sage and how to use them. Next, I will compare Sage's functionality with Magma's functionality. In particular, some gaps in Sage. The last part is an introduction to Sage development using GitHub and the Trac server.

Victor Flynn
Title: Variations on Chabauty-Coleman I

Abstract: This will be a short introduction to main principles of using classical Chabauty-Coleman as a technique for finding rational points on curves, where the rank of the Jacobian is less than the genus of the curve (note that this will be an introduction to the main ideas of the technique, and will not about any specific implementation).

Immanuel Halupczok
Title: Motivic integration and orbital integrals I

Maurizio Monge
Title: A family of Eisenstein polynomials generating totally ramified extensions, identification of extensions and construction of class fields

Abstract: We present a family of special polynomials generating totally ramified extensions of local field *K*. We prove that each extension is generated by at least a special polynomial, but the number of special polynomials generating one extension *L* is at most the number of conjugates of *L*/*K* in the algebraic closure, and in particular it is unique for Galois extensions. A reduction algorithm is presented, and its study allows to characterize the set of special polynomials in terms of the intermediate extensions. A criterion that can ensure that two polynomials generate non-isomorphic extensions is provided, and describe an algorithm which allows to construct a totally ramified class field, given a suitable description of a norm subgroup.

Fernando Rodriguez Villegas
Title: Zeta functions I

David Roe
Title: Overconvergent modular symbols I

Abstract: I will give an introduction to overconvergent modular symbols, their implementation in Sage, and what remains to be done.

Ander Steele
Title: Overconvergent modular symbols II

Abstract: I'll describe an approach to computing families of modular symbols in the higher slope case. I'll also survey the recent work of Robert Harron, Robert Pollack, et. al. on computations of ordinary families.

Jan Tuitman
Title: A survey of p-adic point counting

Abstract: We will give a broad overview of p-adic methods to compute the zeta function of an algebraic variety.

Tristan Vaccon
Title: p-adic Precision I

Abstract: As you already know, p-adic numbers can usually only be handled with finite precision, which yields the problems of determining the smallest precision needed or the loss of precision per operation. With X. Caruso and D. Roe, we have provided a new method to handle precision over p-adics that relies on differentials and first-order approximation. It provides results that are (essentially) optimals and do not depend on the choice of algorithm. We will present an illustration on how to use this method with the study of the computation of the determinant of a p-adic matrix. We will also present the following application. In a joint work with P.Lairez, we have applied this method for the computation of solutions to some p-adic differential equations with separation of variables. These differential equations were studied as they are used to compute isogenies between elliptic curves.

Jeanine Van Order
Title: Iwasawa theory I

Abstract: I will present an overview of Iwasawa theory starting with the work of Iwasawa on Z_p-extensions of number fields, leading to the study of Iwasawa algebras and their structure theory. I will then present three settings where we know the so-called Iwasawa main conjecture in full: totally real number fields (by Wiles/Mazur-Wiles, cf. Rubin), elliptic curves with complex multiplication (by Coates-Wiles/Yager, cf. Rubin), and modular elliptic curves (by Kato/Rohrlich and Skinner-Urban). Some other recent developments and open problems will be discussed at the end of the lecture.

Chris Wuthrich
Title: Iwasawa theory II

Abstract: I intend to show what sage can do with p-adic L-functions of elliptic curves. Through the known results on the p-adic version of the Birch and Swinnerton-Dyer conjecture this gives results on the Tate-Shafarevich group over **Q**, even for elliptic curves of rank greater than 1. My talk should also include what sage cannot do in this direction.