Workshop on Algorithms in Number Theory and Arithmetic Geometry

Universiteit Leiden

31 July–4 August 2017

Nils Bruin (Simon Fraser University): *A tool for numerically computing period matrices of algebraic Riemann surfaces*

The classical, complex analytic description of Jacobians of algebraic curves arise as complex tori: quotients of $\mathbf{C}^g$ by a maximal rank discrete sublattice. Numerical computation to high precision of these lattices allows for numerical discovery of endomorphisms and isogenies of Jacobian varieties.

General purpose implementations of algorithms to compute these lattices to arbitrary precision were already available in Maple (by van Hoeij-de Koninck) and in Magma for hyperelliptic curves (by van Wamelen), but to our knowledge none based on free open soure software.

We present an implementation that will be available in Sage 8.0. As most other implementations, we essentially use the classical definition to compute the matrix. In order to produce an algorithm that has reasonable performance we make some choices:

- we use Voronoi decompositions to produce a homology basis that has nice numerical stability features
- we use a certified homotopy continuation strategy
- we use Gauss-Legendre numerical integration to obtain reasonable convergence.

We will discuss the implementation and give some interesting examples of how one can use the numerical approximations to discover and/or corroborate geometrical facts. This is joint work with Alexandre Zotine.

Henri Cohen (Université de Bordeaux): *Classical Modular Forms in Pari/GP*

At present, computer packages for working with classical modular forms are available in Magma and in Sage, both based on modular or Manin symbols. I will describe a new and extensive package available in Pari/GP based on trace formulas, including in particular modular forms of weight 1. In addition, we hope to be able to show how to compute Fourier expansions at all cusps (including in the nonsquarefree case), how to evaluate forms even near the real line, and how to compute 1/2-integral weight forms.

Vincent Delecroix (LABRI, Bordeaux): *Volumes, intersection and combinatorics in $\overline{\mathcal{M}_{g,n}}$*

There are at least three family of interesting volumes on $\overline{\mathcal{M}_{0,n}}$ the moduli space of the sphere with n marked points: Deligne-Mostow-Thurston, Masur-Veech and Weil–Petersson. The last two are more generally defined on $\overline{\mathcal{M}_{g,n}}$ the moduli space of Riemann surfaces of genus g.

I will explain some of the combinatorics hidden in these volumes, the link with intersection theory in $\overline{\mathcal{M}_{g,n}}$ and how this can be made effective.

Lassina Dembélé (Max-Planck-Institut für Mathematik, Bonn): *On the compatibility between base change and Hecke action*

In this talk, we will discuss the action of $\mathrm{Gal}(F/E)$ on Hecke orbits of automorphic forms on GL_2. This reveals some compatibility between base change and Hecke action, which has several implications for Langlands functoriality.

Maarten Derickx (Universität Bayreuth): *A-gonalities of curves and the existence of infinitely many points of degree d*

The goal of this talk is to study when a curve C over $\mathbb{Q}$ contains infinitely many points whose field of definition is of degree d over $\mathbb{Q}$. Faltings famous Theorem on subvarieties of abelian varieties with infinitely many rational points implies the following: If a curve has infinitely many points of degree d, then either there exists a function of degree d on C or a certain subvariety of the jacobian called W_d^0 contains a translate of a positive rank abelian variety.

The degree of the smallest degree function on C is called the gonality and it has the following two nice properties. The gonality can only decrease when reducing modulo primes p, and over finite fields it is computable in theory and often also in practice using linear algebra. However the question about containment of a translate of a positive rank abelian variety is more difficult to answer, especially in practice. To solve this problem I introduce a concept called the A-gonality for any abelian variety A that is a quotient of $\mathrm{Jac}(C)$, the Jacobian of C. Taking $A = \mathrm{Jac}(C)$ recovers the standard definition of gonality. The A-gonality can, like the standard definition of gonality, only decrease reducing modulo p and is computable in terms of linear algebra as well. Time permitting an application to degree 9 points on the modular curve $X_1(37)$ will be given.

Tom Fisher (University of Cambridge): *Some algebras associated to genus one curves*

Haile, Han and Kuo have studied certain non-commutative algebras associated to a binary quartic or ternary cubic form. These give an explicit realisation of an isomorphism relating the Weil-Chatelet and Brauer groups of an elliptic curve. I will describe how I expect their constructions to generalise to other genus one curves.

Jean-Pierre Flori (ANSSI, Paris): *Computing embeddings of finite fields*

Let $\mathbb{F}_q$ be a finite field. Given two irreducible polynomials f, g over $\mathbb{F}_q$, with $\deg f$ dividing $\deg g$, the finite field embedding problem asks to compute an explicit description of a field embedding of $\mathbb{F}_q[X]/f(X)$ into $\mathbb{F}_q[Y]/g(Y)$. When $\deg f = \deg g$, this is also known as the isomorphism problem.

This problem, a special instance of polynomial factorization, plays a central role in computer algebra software. We review previous algorithms, due to Lenstra, Allombert, Rains, and Narayanan, and propose improvements and generalizations. Our detailed complexity analysis shows that our newly proposed variants are at least as efficient as previously known algorithms, and in many cases significantly better.

We also implement most of the presented algorithms, compare them with the state of the art computer algebra software, and make the code available as open source. Our experiments show that our new variants consistently outperform available software.

Joint work with Ludovic Brieulle, Luca De Feo, Javad Doliskani and Éric Schost.

Kamal Khuri-Makdisi (American University of Beirut): *Jacobian group operations for typical divisors on curves*

Consider the question of efficiently implementing Jacobian group arithmetic for a curve C of genus g, over a finite field K with very large cardinality $q = |K| \gg g$. Many algorithms to do this are formulated for the "typical" case, which holds for "most" divisors once q is very large; so one is in practice very unlikely to encounter a nontypical divisor. This talk presents an explicit characterization of typical divisors an for arbitrary genus g, with a precise bound on how unlikely a nontypical divisor is over a finite field. The main result is algorithms which succeed if and only if the input is typical, and which therefore provide a certificate that the input was typical in case of success.

Steffen Müller (Universität Oldenburg): *Canonical heights on Jacobians of curves of genus two*

To find explicit generators for the Mordell-Weil group of an abelian variety over a global field, one needs algorithms to compute canonical heights of rational points and to enumerate all rational points of bounded canonical height. In my talk, I will discuss how this can be done efficiently for Jacobians of curves of genus 2. This is joint work with Michael Stoll.

Filip Najman (University of Zagreb): *Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields*

Let n be a positive integer such that the modular curve $X_0(n)$ is hyperelliptic of genus ≥ 2 and such that its Jacobian has rank 0 over $\mathbf{Q}$. We determine all points of $X_0(n)$ defined over quadratic fields, and we give a moduli interpretation of these points. We show that, with finitely many exceptions up to

Q-isomorphism, every elliptic curve over a quadratic field K admitting an n-isogeny is d-isogenous, for some $d \mid n$, to the twist of its Galois conjugate by a quadratic extension L of K; we determine d and L explicitly, and we list all exceptions. This is joint work with Peter Bruin.

Bartosz Naskręcki (University of Bristol/Adam Mickiewicz University): *Hypergeometric motives of low degrees*

In this talk we will discuss the construction of hypergeometric motives as Chow motives in explicitely given algebraic varieties. The class of hypergeometric motives corresponds to Picard-Fuchs equations of hypergeometric type and forms a rich family of pure motives with nice L-functions. Following recent work of Beukers-Cohen-Mellit we will show how to realise certain hypergeometric motives of weights 0 and 2 as submotives in elliptic surfaces. An application of this work is computation of minimal polynomials of hypergeometric series with finite monodromy groups and proof of identities between certain hypergeometric finite sums, which mimic well-known identities for classical hypergeometric series.

Pavel Solomatin (Universiteit Leiden): *On Artin L-functions and Gassmann Equivalence for Global Function Fields*

We will discuss an approach to study arithmetical properties of global function fields via Artin L-functions of Galois representations associated to these fields. In particular we recall and then extend a criteria of two function fields to be arithmetically equivalent in terms of Artin L-functions of representations associated to the common normal closure. We will provide few explicit examples of such non-isomorphic fields and also discuss an algorithm to construct many such examples by using torsion points on elliptic curves. Finally, we will show how to apply our results in order to distinguish two global fields by a finite list of Artin L-functions. This talk is based on the pre-print `https://arxiv.org/pdf/1610.05600.pdf`.

Jeroen Sijsling (Universität Ulm): *Computing endomorphisms of Jacobians*

Let C be a curve over a number field, with Jacobian J, and let $\mathrm{End}(J)$ be the endomorphism ring of J. The ring $\mathrm{End}(J)$ is typically isomorphic with $\mathbf{Z}$, but the cases where it is larger are interesting for many reasons, most of all because the corresponding curves can then often be matched with relatively simple modular forms.

We give a provably correct algorithm to verify the existence of additional endomorphisms on a Jacobian, which to our knowledge is the first such algorithm. Conversely, we also describe how to get upper bounds on the rank of $\mathrm{End}(J)$. Together, these methods make it possible to completely and explicitly determine the endomorphism ring $\mathrm{End}(J)$ starting from an equation for C, with acceptable running time when the genus of C is small.

This is joint work with Edgar Costa, Nicolas Mascot, and John Voight.

Jan Tuitman (KU Leuven): *Computing zeta functions of smooth projective hypersurfaces*

We will first give a survey of methods to compute the zeta function of higher dimensional algebraic varieties over finite fields and then talk about a recent algorithm of ours that has the best known complexity for (almost all) smooth projective hypersurfaces.

Christian Wuthrich (University of Nottingham): *Numerical modular symbols*

Given an elliptic curve E over the rationals, the modular symbol attached to E is a map that sends a rational r to the integral from $i\infty$ to r of the differential corresponding to E on the upper half plane divided by the Neron period of E. These symbols $[r]$ are known to be rational numbers. All current implementations start by computing the space of all modular symbols of a given level and then use Hecke operators to cut out the symbol associated to E. Instead one can also compute a numerical approximation of the integral to a proven error bound. With a few tricks, this results in an asymptotically faster algorithm.