CARL VON OSSIETZKY universität OLDENBURG
FAKULTÄT V
MATHEMATIK UND NATURWISSENSCHAFTEN

# Workshop Arithmetic Geometry and Computer Algebra

Oldenburg,
29.06.2017 – 01.07.2017

## Organizers

Florian Heß, Steffen Müller, Andreas Stein

IfM INSTITUT FÜR MATHEMATIK

# Schedule

| **Thursday** | **29.06.2017** |
|---|---|
| 08:30 - 09:20 | Registration |
| 09:20 - 09:30 | Opening |
| 09:30 - 10:30 | John Voight: Semi-arithmetic points on elliptic curves |
| 10:30 - 11:00 | Coffee break |
| 11:00 - 11:30 | Jennifer Balakrishnan: Computing Coleman integrals I |
| 11:30 - 12:00 | Jan Tuitman: Computing Coleman integrals II |
| 12:00 - 15:00 | Lunch & discussion |
| 15:00 - 16:00 | Nils Bruin: Models of genus 2 curves with full level 3 structure |
| 16:00 - 17:00 | Poster session & coffee break |
| 17:00 - 18:00 | Elisa Lorenzo Garcia: Computing twists of hyperelliptic curves |
| **Friday** | **30.06.2017** |
| 09:30 - 10:00 | Pascal Molin: Recent developments in Pari/GP |
| 10:15 - 10:45 | Marc Masdeu: Arithmetic geometry and Sage: an optimistic account |
| 10:45 - 11:15 | Coffee break |
| 11:15 - 11:45 | Steve Donnelly: Recent developments in arithmetic geometry in MAGMA |
| 12:00 - 12:30 | Bill Hart: Nemo: Computer algebra in Julia |
| 12:30 - 15:30 | Lunch & discussion |
| 15:30 - 16:30 | Mike Jacobson: Improved Divisor Arithmetic for Low-Genus Hyperelliptic Curves |
| 16:30 - 17:00 | Coffee break |
| 17:00 - 18:00 | David Kohel: Local methods in geometry |
| 19:00 - open | Dinner at “Zum Drögen Hasen” |

| **Saturday** | **01.07.2017** |
|---|---|
| 09:30 - 10:30 | Andrew Sutherland: Computing $L$-series of genus 3 curves |
| 10:30 - 11:00 | Coffee |
| 11:00 - 12:00 | Tim Dokchitser: Models of curves |
| 12:00 - 13:45 | Lunch & discussion |
| 13:45 - 14:15 | Nicolas Mascot: Modular curves, modular Galois representations and lightly ramified $\mathrm{GL}_2$-fields |
| 14:30 - 15:30 | Peter Bruin: On explicit computations with modular Galois representations |

# Venue

All talks will take place at Carl von Ossietzky Universität Oldenburg in building W1, Lecture Hall W1 0-015. Building W1 is part of Campus Wechloy.

For discussions, room W1 2-213 can also be used on Thursday (after 1PM), Friday (after 1PM), and on Saturday (all day).

The poster session will be in the main lobby of building W1.

# Abstracts

**Speaker**: Jennifer Balakrishnan (Boston University) and Jan Tuitman (KU Leuven)

**Title**: Computing Coleman integrals I and II

**Abstract**: We'll give a survey of explicit Coleman integration on curves via recent algorithms in point-counting and present some applications of Coleman integrals in arithmetic geometry. We'll also describe some new computations on curves of genus 3.

---

**Speaker**: Nils Bruin (Simon Fraser University)

**Title**: Arithmetic aspects of the Burkhardt quartic

**Abstract**: The Burkhardt quartic is a 3-dimensional projective hypersurface of degree 4 with many special properties that are classically known. For instance, its singular locus consists of 45 nodal singularities, and it has a particularly large projective automorphism group. It also has a modular interpretation: it parametrizes abelian surfaces with full level 3 structure. It is also known that the surface is birational to $\mathbb{P}^3$ over the complex numbers.

We look at several arithmetic questions concerning the Burkhardt quartic: We show that the threefold is already rational over $\mathbb{Q}$ (Baker's original parametrization really required cube roots of unity). The exact parametrization also allows us to compute the zeta function of the various reductions (previously, this was only done for primes congruent to 1mod3).

We also look at the moduli interpretation and find an equation for an (almost) universal genus 2 curve with full level structure on its Jacobian, and find a particularly explicit description of how the level structure arises from the geometry of the Burkhardt quartic.

This is joint work with Brett Nasserden.

**Speaker**: Peter Bruin (Leiden Universiteit)

**Title**: On explicit computations with modular Galois representations

**Abstract**: The aim of this talk is to describe a number of aspects of computing with Galois representations with coefficients in finite fields. First, I will explain how one can write down such representations explicitly in terms of "dual pairs of algebras". Next, I will sketch how to compute such dual pairs for Galois representations attached to Hecke eigenforms over finite fields. Finally, I will show a few examples of explicit computations in this setting.

---

**Speaker**: Tim Dokchitser (University of Bristol)

**Title**: Models of curves

**Abstract**: I would like to explain how ideas from toric and tropical geometry can be used to construct regular and semistable models of curves over discrete valuation rings.

---

**Speaker**: Steve Donnelly (University of Sydney)

**Title**: Recent developments in arithmetic geometry in MAGMA

**Abstract**: I will draw attention to some areas where MAGMA has significantly gained capability. More generally, I will talk about how to make good use of MAGMA in the current environment.

**Speaker**: Bill Hart (TU Kaiserslautern)

**Title**: Nemo: Computer algebra in Julia

**Abstract**: I will demonstrate a new package called Nemo.jl written in the Julia programming language (and C), for generic basic arithmetic, and a related project called Singular.jl for accessing Singular functionality from the Julia language. I will explain some of the design decisions we have made, discuss the importance and use of Jit compilation and the Julia type system for the project and detail some of the fast basic arithmetic I've been implementing as a foundation for future projects.

---

**Speaker**: Mike Jacobson (University of Calgary)

**Title**: Improved Divisor Arithmetic for Low-Genus Hyperelliptic Curves

**Abstract**: The most efficient algorithms for arithmetic in the Picard group of a low-genus hyperelliptic curve are given by explicit formulas, where the group operations are expressed as an optimized sequence of field operations as opposed to arithmetic with polynomials. In this talk, we present improved explicit formulas for genus 2 imaginary hyperelliptic curves and genus 3 real hyperelliptic curves defined over finite fields. Our improvements are realized by identifying the best features of previous formulas and combining them in a novel way. In addition, we discuss on-going work on identifying families of genus 2 curves with fast $l$-tupling for $l = 2, 3, 5, 7$.

**Speaker**: David Kohel (Université d'Aix-Marseille)

**Title**: Local methods in geometry (Formal schemes and local methods in computational algebraic geometry)

**Abstract**: The objective of computational algebra is to represent a mathematical object and its associated problems in an equivalent category in which the main questions — equality, isomorphism, existence of morphisms — are effectively and efficiently computable.

Algebraic geometry concerns the solutions to polynomial systems, whose morphisms are polynomial or rational polynomial maps. Often one works locally, passing to an affine subvariety to capture global behavior on a (Zariski) open neighborhood. Already, in this description, we identify two distinguished categories: algebraic schemes with morphisms and the same schemes equipped with rational maps. When restricting to the subcategory of nonsingular projective curves, these two categories coincide, and we exploit this equivalence by representing a morphism by a rational map which determines it. More generally, questions of isomorphism and existence of morphisms have different answers in the two categories.

Often this notion of localization is still too coarse, and we want to develop tools to work locally in a finer topology. This suggests the need to develop the computational tools for working in a category of formal algebraic schemes. We motivate the approach through the category of formal schemes by research problems for which the passage to a category of formal schemes provides an efficient solution.

**Speaker**: Elisa Lorenzo Garcia (Université Rennes I)

**Title**: Computing twists of hyperelliptic curves

**Abstract**: We will discuss an efficient algorithm for computing equations of twists of hyperelliptic curves of arbitrary genus and over any separable field (of characteristic different from 2). We will illustrate the algorithm by explicitly showing some interesting examples. This algorithm together with my results for computing twists of non-hyperelliptic curves provide algorithms for computing the twists equations of any curve. This is joint work with Davide Lombardo.

---

**Speaker**: Nicolas Mascot (University of Warwick)

**Title**: Modular curves, modular Galois representations and lightly ramified $\mathrm{GL}_2$-fields

**Abstract**: We will show how Khuri-Makdisi's algorithm can be adapted to compute efficiently in the Jacobian of modular curves, and how this can be used to compute explicitly Galois representations attached to modular forms. As an application, we will see how to find polynomials for number fields of Galois group $\mathrm{GL}_2$ and $\mathrm{PGL}_2$ whose discriminant is particularly small.

**Speaker**: Marc Masdeu (Universitat Autònoma de Barcelona)

**Title**: Arithmetic geometry and Sage: an optimistic account

**Abstract**: I will give a (necessarily short, and hopefully incomplete) overview of what functionality related to arithmetic geometry is currently included in Sage. With the remaining time, I will explain why I believe that Sage is great when doing research in number theory and/or arithmetic geometry.

---

**Speaker**: Pascal Molin (Université Paris VII)

**Title**: Recent developments in PARI/GP

**Abstract**: We will make a tour of some recent additions to PARI/GP. In particular we will present remarkable new features for computing with modular forms and $L$-functions.

**Speaker**: Andrew Sutherland (MIT)

**Title**: Computing L-series of genus 3 curves

**Abstract**: I will discuss the practical implementation of average-polynomial time algorithms to approximate the L-function of a genus 3 curve $X/\mathbb{Q}$ by computing its Dirichlet coefficients $a_n$ for all $n$ up to a given bound $B$ in time $O(B(\log B)^3)$, where $B$ is assumed to be on the order of the square root of the conductor of the Jacobian of $X$ (or larger).

There are three distinct cases to consider, depending on whether $X$ is hyperelliptic (over $\mathbb{Q}$), a degree-2 cover of a pointless conic, or a smooth plane quartic.

This is joint work with (various combinations of) Andy Booker, David Harvey, Maike Massierer, and David Platt.

---

**Speaker**: John Voight (Dartmouth)

**Title**: Semi-arithmetic points on elliptic curves

**Abstract**: We present a method for constructing points on elliptic curves defined over number fields, combining the theory of Belyi maps and quaternionic Shimura varieties – our method generalizes the construction of Heegner points arising from classical modular curves. We present computations of these points which show that in some cases, they generate a subgroup of points with rank greater than one.

# Lunch

There are several near-by options for lunch/dinner:

- Cafeteria at Campus Wechloy (this is where the talks are): you can choose between two main dishes (one is always vegetarian); closed on Saturday; lunch only.
- Cafeteria at Campus Haarentor: the cafeteria at the other campus can be reached by walking (about 10–15 minutes), or by bus (5 minutes, 3 stops); they offer a larger variety of main dishes (including vegetarian & vegan options); also closed on Saturday and lunch only.
- Restaurant Ali Baba: Turkish cuisine; can be reached by walking (about 15 minutes), or by bus (5 minutes, 3 stops); mainly non-vegetarian; open for lunch and dinner.
- Moto Kitchen: Sushi & Thai cuisine; can be reached by walking (about 10 minutes), or by bus (3 minutes, 2 stops); open for lunch and dinner.
- Finca & Bar Celona: Mainly tapas, pasta & burgers, can be reached by walking (about 15 minutes); open all day.

# Workshop Dinner

The workshop dinner will take place at the restaurant "Zum Drögen Hasen" (5 minute walk from Campus Wechloy) on Friday, 30.06. starting at 19:00.

# Sponsors



Gefördert von


UNIVERSITÄTSGESELLSCHAFT
OLDENBURG e.V.