UNIVERSITÄT BAYREUTH

CHAIR OF COMPUTER ALGEBRA

CA@BT

Workshop Program ‘Rational Points 2025’

Sunday, July 27

	Arrival
14:00–∼18:00	*Reception is open*
from ∼18:00	*Keys available at the restaurant*
18:30–21:30	*Dinner*

Monday, July 28

08:00–09:15	*Breakfast*
09:20–09:30	Michael Stoll: *Opening and Welcome*
09:30–10:00	Nils Bruin: **2-isogenies on Jacobians of curves of genus 3**
10:15–10:45	Brendan Creutz: **Adelic Mordell-Lang and the Brauer-Manin obstruction**
10:45–11:15	*Coffee*
11:15–12:15	Jef Laga: **Reduction theory and heights of rational points**
12:30–13:30	*Lunch*
15:00–16:00	*Coffee*
16:00–16:45	Pip Goodman: **Semistable abelian varieties over $\mathbb{Q}$ which have good reduction outside of 29**
17:00–17:30	Jack Thorne: **Kummers, spinors, and heights**
17:45–18:15	Sudip Pandit: **Explicit Mordell–Lang bound for curves in low rank**
18:30–19:30	*Dinner*

Tuesday, July 29

08:00–09:15	*Breakfast*
09:30–10:30	María Inés de Frutos Fernández: **Arithmetic Geometry in the Lean Proof Assistant**
10:30–11:15	*Coffee*
11:15–12:15	John Voight: **The generalized Fermat equation and Pochhammer Pryms**
12:30–13:30	*Lunch*
15:00–16:00	*Coffee*
16:00–16:45	Jan Steffen Müller: **Quadratic Chabauty over number fields and 3-adic Galois representations**
17:00–17:30	Jen Balakrishnan: **Algebraic mock rational points on curves**
17:45–18:15	Drew Sutherland: **A database of genus 2 curves of small conductor**
18:30–19:30	*Dinner*
20:00–?	**Open Problems**

Wednesday, July 30

08:00–09:15	*Breakfast*
09:30–10:30	Kate Stange: **Local-to-global in thin orbits**
10:30–11:15	*Coffee*
11:15–12:15	Jerson Caro: **Counting and finding rational points on surfaces**
12:30–13:30	*Lunch*
	Free Afternoon, *Coffee* and *Dinner* on request

Thursday, July 31

08:00–09:15	*Breakfast*
09:30–10:30	Davide Lombardo: **More about the p-adic images of Galois for elliptic curves over $\mathbb{Q}$**
10:30–11:00	*Coffee*
11:00–11:30	Carlo Pagano: **2-descent and additive combinatorics**
11:45–12:15	Maarten Derickx: **Answering a question of Krumm about the imaginary quadratic points of $Y_1(16)$**
12:30–13:30	*Lunch*
15:00–16:00	*Coffee*
16:00–16:45	Filip Najman: **Torsion of elliptic curves over quartic fields**
17:00–17:30	Elvira Lupoian: **Torsion subgroups of modular Jacobians**
17:45–18:15	David Angdinata: **Rational points on elliptic curves in Lean**
18:30–19:30	*Dinner*

Friday, August 1

08:00–09:15	*Breakfast*
09:30–10:30	Cecília Salgado: **Hilbert Property: From K3 Surfaces to Campana Points**
10:30–11:15	*Coffee*
11:15–12:15	Katharine Woo: **On Manin's conjecture for Châtelet surfaces**
12:30–13:30	*Lunch*
15:00–16:00	*Coffee*
16:00–16:45	Margherita Pagano: **Transcendental Brauer-Manin obstruction on surfaces**
18:30–19:30	*Dinner*

Saturday, August 2

07:30–09:30	*Breakfast*
	Departure

Abstracts

Nils Bruin: **2-isogenies on Jacobians of curves of genus 3**

For elliptic curves, 2-isogenies have a very explicit description and on Jacobians of curves of genus 2*, we have Richelot's description of* 2*-isogenies. In genus* 3 *this fails for a rather fundamental reason: If we take a quotient of a Jacobian of a curve of genus* 3 *by a maximal isotropic subgroup of the* 2*-torsion then we do obtain a principally polarized abelian variety of dimension* 3*, but such a variety is only guaranteed to be a quadratic twist of a Jacobian.*

Donagi-Livné and Lehavi-Ritzenthaler describe an elaborate construction using various Prym varieties to obtain the genus 3 *curve generating that Jacobian. With some additional work, we can also extract the quadratic twist. This allows us to generate various interesting examples of isogenous abelian* 3*-folds over* $\mathbb{Q}$*.*

This is joint work with Damara Gagnier.

Brendan Creutz: **Adelic Mordell-Lang and the Brauer-Manin obstruction**

For a closed subvariety X *of an abelian variety over a number field, the Mordell-Lang conjecture proved by Faltings has the following consequence: The set of rational points of* X *are contained in a finite union of translates of abelian subvarieties contained in* X*.*

The adelic Mordell-Lang conjecture is a strengthening of this which asserts that the set of adelic points of X *which are orthogonal to the Brauer group are contained in a finite union of translates of abelian subvarieties contained in* X*. I will discuss ongoing work with Felipe Voloch around this conjecture and its consequences for the Brauer-Manin obstruction. We generalize some results of Stoll and Poonen-Voloch from the case that* X *contains no translate of a positive dimensional abelian subvariety to the case of arbitrary closed subvarieties.*

Jef Laga: **Reduction theory and heights of rational points**

Given an action of an arithmetic group on a set, reduction theory is concerned with finding representatives whose coefficients are small. It is a powerful tool in computational number theory, with lattice reduction being a prominent example. I will explain how reduction theory can also be a powerful theoretical tool, by relating it to heights of rational points in certain situations, which leads to a proof of the following statement: for 100% of monic odd hyperelliptic curves of genus g*, its Jacobian variety has no nonzero points of small height (in a precise sense).*

This is joint work with Jack Thorne.

Pip Goodman: **Semistable abelian varieties over** $\mathbb{Q}$ **which have good reduction outside of 29**

In joint work Francesco Campagna, we classify all such abelian varieties. The main difficulty in doing so is due to the existence of a simple group scheme V *of order* 4 *which is everywhere locally reducible (but globally irreducible). This makes it hard to classify extensions of* V *by itself. A key step in being able to do so comes from proving the failure of a type of local–global principle for finite flat group schemes. In this talk I will give an introduction to finite flat group schemes and outline a proof of the above.*

Jack Thorne: **Kummers, spinors, and heights**

Let $f(x) = x^{2g+1} + c_1x^{2g} + \cdots + c_{2g+1}$ *be a polynomial of nonzero discriminant, and let* J *denote the Jacobian of the odd hyperelliptic curve* $C\colon y^2 = f(x)$*. I will explain how the morphism* $|2\Theta|\colon J \to \mathbb{P}^{2^g-1}$ *may be described explicitly using the theory of pure spinors, and how this description may be applied to the theory of heights.*

Sudip Pandit: **Explicit Mordell–Lang bound for curves in low rank**

In this talk, we will discuss the Buium–Coleman method to study the Mordell–Lang conjecture for curves, i.e., studying the points on a curve that lie in a finite rank subgroup inside the Jacobian. Under the assumption that the rank is less than the genus, we can prove the conjecture, obtaining an explicit bound. As a corollary, we can also derive a p-adic proof of "Mordell implies Mordell–Lang". This is joint work with Netan Dogra.

María Inés de Frutos Fernández: **Arithmetic Geometry in the Lean Proof Assistant**

Mathematical formalization is the process of digitizing mathematical definitions and results using a "proof assistant", a software capable of checking logical statements against a set of inference rules and some basic axioms. In recent years, the community of mathematicians working on formalization has grown rapidly and has reached milestones that demonstrate the ability to formalize results at the frontier of knowledge. Proof assistants have applications to mathematical research, teaching, and communication.

After a brief introduction to formalization and the proof assistant Lean, I will give an overview of some definitions and results from arithmetic geometry that have been formalized in Lean's mathematical library Mathlib, or in projects building over it.

John Voight: **The generalized Fermat equation and Pochhammer Pryms**

We give an explicit moduli interpretation to the generalized Fermat equation $x^a + y^b = z^c$ *by associating a family of abelian varieties which we call Pochhammer Prym varieties. Over the complex numbers, we recover the modular embedding of Cohen and Wolfart defined by hypergeometric functions; our construction via Hurwitz stacks provides naturally defined arithmetic models. This is joint work with Robert Kucharczyk.*

Jan Steffen Müller: **Quadratic Chabauty over number fields and 3-adic Galois representations**

The quadratic Chabauty method is an instance of Kim's nonabelian Chabauty program that can be used to compute rational points on some curves of genus > 1 *over the rationals in practice. I will discuss joint work with Balakrishnan, Betts, Hast and Jha that extends this to certain (modular) curves over number fields. As an application, we completed the characterisation of* 3*-adic Galois representations of non-CM elliptic curves.*

Jen Balakrishnan: **Algebraic mock rational points on curves**

For curves over the rationals satisfying certain hypotheses, Kim's nonabelian Chabauty program associates various finite sets of p-adic points, known as the Chabauty–Kim sets. We describe the computation of the Chabauty–Kim sets in various settings and examine the mock rational points (those finitely many points that are not rational) that may arise in these sets, with a particular interest in those points that are algebraic. Throughout, we present a number of examples.

Drew Sutherland: **A database of genus 2 curves of small conductor**

The LMFDB currently contains a database of genus 2 *curves over* $\mathbb{Q}$ *that includes* 66 158 *curves and associated invariants, including information about rational points and the Mordell-Weil group of the Jacobian. This database was the result of a large scale search for genus* 2 *curves with absolute minimal discriminant bounded by* 10^6. *In recent joint work with Andy Booker we constructed a new database of genus* 2 *curves over* $\mathbb{Q}$ *with conductor bounded by* 2^{20}, *which includes the genus* 2 *curves currently in the LMFDB along with more than* 6 *million new curves. I will describe the construction of this database and some of its features.*

Kate Stange: **Local-to-global in thin orbits**

I'll discuss a number of examples of local-to-global conjectures in thin orbits, including Apollonian circle packings and Zaremba's conjecture. These are questions of whether congruence (mod n) obstructions in integer orbits of thin groups or semigroups control the global orbit: does one obtain all sufficiently large integers subject to these congruences? In analogy to the Diophantine setting, in some cases this principle fails and there are obstructions arising from reciprocity laws.

Jerson Caro: **Counting and finding rational points on surfaces**

A celebrated result of Coleman gives an explicit version of Chabauty's theorem, bounding the number of rational points on curves over number fields via the study of zeros of p-adic analytic functions. While many developments have extended and refined this result, obtaining analogous explicit bounds for higher-dimensional subvarieties of abelian varieties remains a major challenge.

In this talk, I will sketch the proof of such an explicit bound for surfaces contained in abelian varieties — a step toward a higher-dimensional Chabauty–Coleman method. This is joint work with Héctor Pastén.

I will also describe an application of this method to a computational problem: determining an upper bound for the number of unexpected quadratic points on hyperelliptic curves of genus 3 defined over $\mathbb{Q}$. I will illustrate the method through an explicit example where this set can be computed. This is joint work with Jennifer Balakrishnan.

Davide Lombardo: **More about the p-adic images of Galois for elliptic curves over $\mathbb{Q}$**

I will describe ongoing joint work with Matthew Bisatt and Lorenzo Furio in which we study the possible images of the p-adic Galois representations attached to elliptic curves over the rationals. For $p > 37$, we show that the only possibilities are the inverse images in $\mathrm{GL}_2(\mathbb{Z}_p)$ of a non-split Cartan modulo p^n for some $n \geq 1$. This requires ruling out both the proper subgroups of the non-split Cartan modulo p and certain exotic groups of level p^2. To handle the latter, we borrow tools from p-adic Hodge theory to give a very explicit description of the p^2-torsion representation for elliptic curves over $\mathbb{Q}_p$ in the most complicated case (bad, potentially good supersingular reduction).

Carlo Pagano: **2-descent and additive combinatorics**

I will explain two recent joint works with Peter Koymans, where we introduced a new method to construct curves with positive but constrained rank over general number fields. In the former (in 2024) we used this to settle Hilbert's 10th problem for any finitely generated infinite ring. In the latter (in 2025) we used these ideas to show that every number field has an elliptic curve of rank exactly equal to 1. I will explain the proofs, present some open questions, and, if time allows, discuss some further application of the second result to the definability of arithmetic structures.

Maarten Derickx: **Answering a question of Krumm about the imaginary quadratic points of $Y_1(16)$**

Twelve years ago David Krumm observed using explicit computations that if the modular curve $Y_1(16)$ has an imaginary quadratic point, then the class number of the quadratic field tends to be divisible by 10. He found only one exception to the divisibility by 10 for such points, and asked whether that one exception is indeed the only one. In this talk I will prove that David Krumm's question has a positive answer. The core of the argument consists of transporting an explicit element of $J_1(16)(\mathbb{Q})$ of order 5 to the class group of the imaginary quadratic field. There are some obstructions to doing this; using the structure of the minimal regular model of $X_1(16)$ allows one to one to study these obstructions. This part of the proof can also be interpreted as doing a μ_5-descent while only using information on the 5-part of the class group of the imaginary quadratic field.

Filip Najman: **Torsion of elliptic curves over quartic fields**

We determine all the possibilities for the torsion group $E(K)_{\text{tor}}$ where K ranges over all quartic number fields and E ranges over all elliptic curves over K. We show that there are no sporadic torsion groups, or in other words, that all torsion groups either do not appear or they appear for infinitely many non-isomorphic elliptic curves E. Proving this requires showing that numerous modular curves $X_1(m, n)$ have no non-cuspidal degree 4 points. We deal with almost all the curves using one of three methods: a method for the rank 0 cases requiring no computation; the Hecke sieve, a local method requiring computer-assisted computations; and the global method, an argument for the positive rank cases also requiring no computation. This is joint work with Maarten Derickx.

Elvira Lupoian: **Torsion subgroups of modular Jacobians**

In 1976 Mazur proved that the rational torsion subgroup of the Jacobian of $X_0(N)$, with N prime and at least 5, is generated by the equivalence class of the difference of the two cusps. In this talk, we'll discuss a generalisation of this result for the Jacobian of the modular curves lying between $X_0(N)$ and $X_1(N)$.

David Angdinata: **Rational points on elliptic curves in Lean**

I will talk about the state of elliptic curves in the Lean proof assistant and what to expect in the next few years.

Cecília Salgado: **Hilbert Property: From K3 Surfaces to Campana Points**

Let X be a smooth projective variety over a number field k, and let D_m be a divisor on X with multiplicities encoded by a weight vector m. Campana points on X are rational points that are integral with respect to this weighted boundary divisor. They generalise classical integral points and allow one to interpolate between the theories of rational and integral points in a systematic way.

Several conjectures and theorems about rational points on varieties have natural analogues in the Campana setting. For example, it is conjectured that if the pair (X, D_m) is log Fano, then the set of Campana points is Zariski dense—echoing the expected potential density of rational points on Fano varieties.

In this talk, we explore a finer arithmetic question, namely of whether the set of Campana points on log Fano pairs is not thin (over some finite extension of k), i.e., satisfies the (potential) Hilbert property. We focus on the case of log Fano pairs of the form $(\mathbb{P}^2, D_m)$, and discuss how their (potential) Campana Hilbert property is connected to the classical (potential) Hilbert property for K3 surfaces over number fields. As a result, we obtain the (potential) Hilbert property for several open cases of logFano pairs $(\mathbb{P}^2, D_m)$.

This is based on work in progress with Marta Pieropan and Soumya Sankar.

Katharine Woo: **On Manin's conjecture for Châtelet surfaces**

We resolve Manin's conjecture for all Châtelet surfaces over $\mathbb{Q}$ (surfaces given by equations of the form $x^2 + ay^2 = f(z)$) — we establish asymptotics for the number of rational points of increasing height. The key analytic ingredient is estimating sums of Fourier coefficients of modular forms along polynomial values.

Margherita Pagano: **Transcendental Brauer-Manin obstruction on surfaces**

In this talk, after brief introduction to the Brauer–Manin obstruction and its use in the study of rational points, we will focus on how the reduction of a variety modulo a prime p can be used to study the Brauer–Manin obstruction. In particular, we will explore the role of primes of good reduction in this context.