Program

Modular curves and Applications of AI to Number theory

September 14–18, 2026
Grand Hotel 4 Opatijska Cvijeta, Opatija, Croatia

Contents

Schedule

In addition to the invited and contributed talks, the programme features a **problem session**, where everyone is warmly welcome to present their own open problems; **lightning talks**; and a **open discussion on norms on the use of AI in mathematics**. Some topics we will discuss include:

- AI disclosure — how much disclosure is needed;
- the issue of credit, and appropriate credit;
- how can we give problems to graduate students in the age of AI?
- selling / giving problems to AI companies;
- "scooping" other people with AI, or working on a problem that you may know someone else is working on;
- refereeing with AI;
- hiring and tenure procedures in the age of AI;
- privacy.

Monday *Sep 14*

8:50–9:20	Registration
9:25–9:30	Introduction
9:30–10:15	Pierre Parent
10:25–10:45	Guido Lido
10:45–11:15	*Coffee break*
11:15–12:00	Maarten Derickx
12:10–12:30	Ivan Novak
12:30–14:15	*Lunch break*
14:15–15:00	Bartosz Naskręcki
15:10–16:00	Discussion about AI in math

Tuesday *Sep 15*

9:50–10:35	Kathrin Bringmann
10:35–11:15	*Coffee break*
11:15–12:00	Álvaro Lozano-Robledo
12:10–12:30	Nikola Adžaga
12:30–14:30	*Lunch break*
14:30–14:50	Freddy Saia
15:00–16:00	Problem session
16:00–16:45	Ken Ono *online*

Wednesday *Sep 16*

9:30–10:15 Davide Lombardo

10:25–10:45 Francesc Bars Cortina

10:45–11:15 *Coffee break*

11:15–12:00 Sachi Hashimoto

12:10–12:30 Lightning talks:

- Sanda Bujačić Babić
- Zrinka Franušić
- Ana Jurasić

12:30 Conference photo

12:30– *Free afternoon*

Thursday *Sep 17*

9:30–10:15 Daeyeol Jeon

10:25–10:45 Yongjae Kwon

10:45–11:15 *Coffee break*

11:15–11:35 David Kurniadi Angdinata

11:45–12:05 Takafumi Miyazaki

12:05–14:15 *Lunch break*

14:15–15:00 Abbey Bourdon

15:10–15:30 Marin Varivoda

Friday *Sep 18*

9:30–10:15 Alexey Pozdnyakov

10:25–10:45 Maciej Ulas

10:45–11:15 *Coffee break*

11:15–12:00 Domagoj Vlah

12:00 *End of conference*

Invited talks

Abbey Bourdon

Wake Forest

Polynomial bounds on torsion for elliptic curves with rational j-invariant

In 1996, Merel showed that for any elliptic curve defined over a number field F of degree d, the size of the torsion subgroup is bounded by a constant $B(d)$ that depends only on d. It is conjectured that one can choose $B(d)$ to be polynomial in the degree d. For the special class of elliptic curves with j-invariant in $\mathbb{Q}$, polynomial bounds were first established by Clark and Pollack in 2018. In this talk, I will discuss recent improvements to these bounds that are essentially optimal for the exponent of the torsion subgroup.

Kathrin Bringmann

Köln

Ramanujan-type identities and Jacobi–Eichler integrals

Ramanujan discovered remarkable transformation formulas involving Lambert series, Bernoulli numbers, and odd zeta values. I will discuss a generalization due to Lim and explain how it leads naturally to Jacobi analogues of classical Eichler integrals. We construct explicit non-holomorphic completions of these functions and show that they are singular harmonic Maass–Jacobi forms. Their specializations at torsion points yield harmonic and sesquiharmonic Maass forms, while differential operators connect the resulting family to Eisenstein series. I will conclude with extensions to several elliptic variables and some open questions. This is joint work with Rajat Gupta and Badri Pandey.

Maarten Derickx

Zagreb

Open problems on modular curves

In this talk I will discuss several open questions about algebraic point on modular curves. I will especially focus on questions where I think it should be possible to make progress in the near future.

Sachi Hashimoto

Colorado

Atkin-Lehner Quotients

I will discuss rational points on the star curves $X_0^*(N)/W(N)$, the quotients of$X_0(N)$ by the full Atkin–Lehner group, at squarefree level. Their noncuspidal rational points parametrize Q-curves, and Elkies conjectured that for sufficiently large level, every rational point is either cuspidal or CM. We call the remaining rational points exceptional. In joint work with Eran Assaf and Ari Shnidman, we find new exceptional points in genera 3 and 4, and give evidence for an effective Elkies conjecture. We also study geometric explanations for these exceptional points. If time permits, I will also discuss related work with Assaf on the classification of hyperelliptic Atkin–Lehner quotients of Shimura curves $X_0(D, N)$.

Daeyeol Jeon

Kongju

D-Elliptic Modular Curves $X_0(N)$

We study the existence of rational morphisms of a prescribed degree D from the modular curve $X_0(N)$ to elliptic curves over $\mathbb{Q}$. We develop a computational method based on degree pairings on $\mathrm{Hom}_{\mathbb{Q}}(J_0(N), E)$, which gives positive definite quadratic forms representing possible degrees of such morphisms. To handle elliptic curves in the same rational isogeny class, we combine these quadratic forms with a lifting criterion on homology lattices, implemented using Smith normal form. We also use Shimura subgroups to obtain quadratic forms describing all possible degrees in many cases. As an application, we determine all D-elliptic modular curves $X_0(N)$ for $D = 3, 4, 5$. This is joint work with Maarten Derickx, Yongjae Kwon, and Petar Orlić.

Davide Lombardo

Pisa

Rational points on modular curves & generalised Fermat equations

The ℓ-adic case of Mazur's "Program B" seeks to determine all possible images of the ℓ-adic Galois representations attached to non-CM elliptic curves over $\mathbb{Q}$. In this talk, I will describe recent progress on this problem for $\ell = 7$, based on a surprising correspondence between rational points on modular curves and primitive integer solutions to certain generalised Fermat equations, such as $a^2 + 28b^3 = 27c^7$. We show that these Diophantine equations can be reduced to finding the rational points on a finite collection of genus-3 curves. As a consequence, we determine the rational points on a modular curve of genus 69 and establish that the 7-adic Galois images of elliptic curves over $\mathbb{Q}$ are determined by their reduction modulo 7^2. This is joint work with Lorenzo Furio.

Álvaro Lozano-Robledo

University of Connecticut

The Geometric Congruence Subgroup

In this talk we will construct a subgroup $\Gamma(X)$ of $\mathrm{SL}(2, \mathbb{Z}[X])$, which we call the geometric congruence subgroup, such that $\Gamma(X)|_{X=p} = \Gamma(p)$, for every prime p. The proof of this equality had evaded the author for over a decade, but ChatGPT 5.4 was able to find a proof using recent results of Vaserstein. We will explain Vaserstein's results, and derive a number of consequences of this construction. This is joint work with Alex Abrams, and Holden Lee.

Bartosz Naskręcki

Poznań

Auto-research in algebra and number theory

I want to explain the new paradigm of auto-research based on my recent experience of work with ECDSA.fail and the classification of finite semigroups of order 6. I will explain both the top results that we achieved and the interesting agentic architecture that was used for two months with each project. I will talk about mathematics done at scale - a new form of mathematical data science.

Ken Ono (online)

University of Virginia and Axiom Math

The secret life of partitions

The partition function $p(n)$ begins with child's play yet touches many corners of mathematics. This talk traces the pursuit of exact information about $p(n)$, from the work of Euler, Hardy–Ramanujan, and Rademacher to a finite algebraic formula (with Bruinier) expressing p(n) as a trace over CM points on $X_0(6)$. We show how this framework yields a conceptual proof of the Ramanujan congruences modulo powers of 5, 7, and 11 through the moduli of elliptic curves. We also present a new theorem (joint with Swaminathan) that $p(n)$ takes both parities infinitely often along the progressions $n = (Dm^2 + 1)/24$, which set the new record for the appearance of odd values improving on the previous bound of Joel Bellaiche, Ben Green, and Kannan Soundararajan.

Pierre Parent

Bordeaux

Equation-free quadratic Chabauty for modular curves: some geometric aspects

After the pioneering work of Minhyong Kim, J. Balakrishnan, N. Dogra, S. Müller, J. Tuitman and J. Vonk, recent years have seen the development of radical improvements of the classical Chabauty method for determining rational points on curves, called "non-abelian Chabauty". Whereas the first formulations relied strongly on p-adic cohomological tools, B. Edixhoven and G. Lido have subsequently proposed a version which is closer in spirit to Chabauty's original geometric intuition.

All versions however have demanded so far explicit equations for the curves to be studied. In a joint project with S. Hashimoto, G. Lido, D. Lombardo and N. Mascot, we formulate the geometric method in moduli terms only, in order to study new examples of modular curves, hoping this will contribute to shed light on the method's possibilities (or limits). We recover in particular the case of the non-split modular curve of level 13 (the "cursed" one). This talk will try to discuss some of the geometric aspects of the method.

Alexey Pozdnyakov

Princeton

On (not) learning the Möbius function

We discuss lower bounds on learning the Möbius or Liouville function with a variety of standard learning techniques, including kernel methods, noisy gradient methods, and correlational statistical query algorithms. In particular, we will see that one can not learn the Möbius function using noisy gradient descent on a fully connected neural network. The emphasis will be on how to formulate such a result and the key ideas that allow you to prove it. We will also see that these results are closely related to counting primes with linear constraints on their digits.

Domagoj Vlah

Zagreb

From chat to a research workflow: sustained mathematical work with project instructions

How can a sequence of interactions with a language model become a continuing research workflow? I describe a practical approach implemented in the ordinary ChatGPT web interface: a short set of project instructions points to a detailed protocol, while files preserve the current state, sources, unresolved claims and next actions. The emphasis is on the functions of these instructions, not a catalogue of prompt clauses. A joint experiment with Matija Kazalicki provides the case study. The original unpublished problem remains unresolved, but the workflow also produced a separate finite-field manuscript. I will explain a translation-averaged counting result whose draft proofs Matija checked without finding errors. The case illustrates both useful continuity and substantial coordination costs. I will relate the method to tool-feedback, context-management and research-agent work, and distinguish natural-language checking from formal proof verification.

Contributed talks

Nikola Adžaga

Zagreb

Quadratic Chabauty on $X_0(N)^*$

Quadratic Chabauty computations for $X_0(N)^*$ are complicated by local height contributions at primes of bad reduction. For squarefree N, we explain a strategy for choosing a correspondence for which all those contributions vanish. We first determine the dual graphs of the special fibers of semistable models of $X_0(N)^*$ at primes of bad reduction. The long cycles in these graphs impose linear conditions our correspondence has to satisfy. Using embeddings of quadratic orders into quaternion algebras, we obtain an upper bound for the number of these conditions; when the genus of $X_0(N)^*$ is greater than one more than this bound, there is enough freedom to choose a suitable correspondence, simplifying quadratic Chabauty computations. As an application, we determine the rational points on several curves $X_0(N)^*$ for which this was not done before. Moreover, as our main result, we show that such a correspondence exists for all but finitely many squarefree levels.

This is joint work with Maarten Derickx and Timo Keller.

Debargha Banerjee

IISER Pune

Cuspidal subgroups associated with non-rational Eisenstein maximal ideals

We are interested in the generalization of Ramanujan-like Eisenstein congruences (congruences between cusp forms and Eisenstein series) for congruence subgroups of the form $\Gamma_0(N)$ with $N \in \mathbb{N}$. We determine the possible primes that can produce Eisenstein congruences. We provide several examples of Eisenstein congruences to substantiate our method. Ribet conjectured ([p. 360, MR3540618]) about these congruences for the square-free level N. Yoo proved the conjecture. For general N, Yoo proved a generalization of the conjecture, under some hypotheses, provided that those ideals are *rational*. We show that the generalization of Ribet's conjecture for certain non-square-free levels N is true even for *non-rational* Eisenstein maximal ideals.

Francesc Bars Cortina

UAB Barcelona

On quotient modular curves by V_5 and rational points

For the classical modular curves $X_0(25M)/\langle w_{25}\rangle$ with M coprime with 5 there is a natural modular automorphism V_5 of order 3 which was not much studied in the literature, see (DOI: 10.1112/mtk.70065, 2026). In the talk, we will present a moduli interpretation of this modular automorphism and properties of the quotient modular curves obtained by quotienting out by V_5. This is a joint work with S. Arpin, T. Dalal, M. Derickx and P. Orlić.

David Kurniadi Angdinata

University of East Anglia

Torsion and Tamagawa numbers over function fields

I compute explicit cancellations between torsion subgroups and Tamagawa products of elliptic curves over global function fields, which gives a lower bound to Birch and Swinnerton-Dyer quotients, and describe my use of large language models to autoformalise them in the Lean theorem prover. This is joint work with Mentzelos Melistas.

Yongjae Kwon

Kongju National University

Degree divisibility for old elliptic quotients of $X_0(N)$

Let $E/\mathbb{Q}$ be the strong Weil curve of conductor M, with modular parametrization $\pi_E\colon X_0(M) \to E$. At level M, optimality gives a natural divisibility property for the degrees of maps from $X_0(M)$ to elliptic curves in the same isogeny class. This talk addresses whether the same divisibility persists for maps from $X_0(N)$, where M divides N.

We prove that, for old elliptic quotients, the minimal-level modular-degree divisibility persists up to an explicit factor involving the Manin constant. In particular, when the Manin constant is one, the degree of π_E divides the degree of every nonconstant map from $X_0(N)$ to an elliptic curve in the same $\mathbb{Q}$-isogeny class.

This is joint work with Daeyeol Jeon (Kongju National University).

Guido Lido

Rome Tor Vergata

Automorphisms of modular curves

In this joint work with Valerio Dose and Pietro Mercuri, we investigate whether a modular curve can have exceptional (non "modular") automorphisms, which are often linked to exceptional points. We prove it does not happen in prime level large enough, and we give a sufficient criterion, which is easy to verify, e.g. with the data available on the LMFDB, for modular curves of composite level.

Takafumi Miyazaki

Gunma University

Applications of Baker's method to purely exponential Diophantine equations with four terms

One of the important unsolved problems in Diophantine number theory is to establish a general method to effectively find all solutions to any given S-unit equation having at least four terms. Although there are so many works contributing to this problem in the literature, most of which handle purely exponential Diophantine equations (ex. $3^x - 2^y = 1, 3^x + 4^y + 5^z = 6^w$), it can be said that all of them solve only finitely many such equations. In this talk, we start reviewing known methods for the ternary case, and discuss how efficiently some of those methods (in particular, Baker's method) can be used to examine the equations with at least four terms. Finally, we study infinitely many purely exponential Diophantine equations with four terms of consecutive bases. Our result states that all solutions to the equation $n^x + (n+1)^y + (n+2)^z = (n+3)^w$ in positive integers n, x, y, z, w with $n \equiv 3 \pmod 4$ are given by $(n, x, y, z, w) = (3, 3, 1, 1, 2), (3, 3, 3, 3, 3)$.

Ivan Novak

Zagreb

Isogeny graphs of elliptic curves in characteristic zero

In this talk, we discuss isogeny graphs of elliptic curves in characteristic 0. The isogeny graph of an elliptic curve E over some field K is the graph whose vertices are elliptic curves K-isogenous to E, and the edges correspond to p-isogenies for prime p. The isogeny graph is a Cartesian product of p-isogeny graphs. We classify, for each prime p, all possible p-isogeny graphs which can appear over some field of characteristic 0 for non-CM elliptic curves. We also discuss questions about growth of isogeny graphs upon field extensions.

Freddy Saia

Lafayette College

Isogenies and exceptional isomorphisms between quotients of modular and Shimura curves

We will discuss the determination of all isogenies between an oft-studied family of Shimura curves, as well as between quotients thereof by subgroups of their Atkin–Lehner involutions. This naturally leads into, and indeed was motivated by, a consideration of isomorphisms between such curves, including those which do not factor through the natural quotient maps from the complex upper half-plane over $\mathbb{C}$. This is joint work with Nikola Adžaga and Oana Padurariu.

Maciej Ulas

Jagiellonian University

On the Diophantine equation $C(x, y) = f(z) + k$

In this note we initiate the study of the title Diophantine equation, where $C \in \mathbb{Z}[x, y]$ is reducible cubic form and $f \in \mathbb{Z}[z]$ of degree 4 satisfies $f(0) = 0$. We prove lower bound for the number of integers k representable by the polynomial $C(x, y) - f(z)$ satisfying $|k| < N$. Moreover, we present computational results concerning the numbers k represented in the form $x^3 + y^3 - z^4$ with $x, y, z \in \mathbb{Z}$.

Marin Varivoda

Zagreb

Torsion groups of elliptic curves that appear infinitely often over septic, octic and nonic fields

We determine the sets $\Phi_\infty(n)$ of abelian groups that occur as torsion groups of infinitely many elliptic curves, up to $\overline{\mathbb{Q}}$-isomorphism, over number fields of degree $n = 7, 8$, and 9. The proof translates the problem into one concerning low-degree points on modular curves $X_1(m, n)$. We construct the infinite families using modular units and eliminate the remaining candidates using finite-field gonality computations, covering arguments, and a specialization argument for W_d^0. The most difficult case is $X_1(37)$ in degree 9, where the Jacobian has positive rank. We handle this case by showing that $W_9^0(X_1(37))$ over $\mathbb{F}_2$ contains no translate of the positive-rank elliptic factor induced by the morphism $X_1(37) \to X_0^+(37)$.