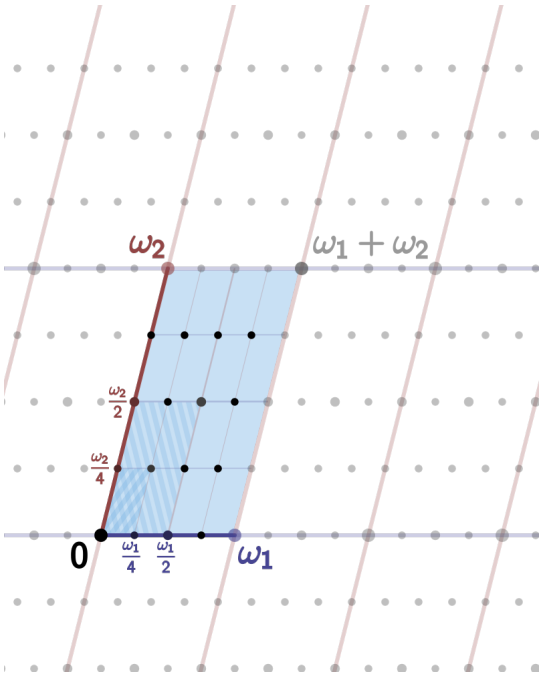
QuantiXLie Center of Excellece
&
Department of Mathematics, Faculty of Science,
University of Zagreb

Book of Abstracts

Modular curves and Galois representations



September 18 – 22, 2023, Zagreb, Croatia

Preface

This brochure consists of the program of presentations and abstracts of papers presented at the *Modular curves and Galois representations of elliptic curves* confernce organized by the *QuantiXLie Center of Excellece* and *Department of Mathematics, Faculty of Science, University of Zagreb*. The purpose of this conference is to bring together experts working on Modular curves and Galois representations attached to elliptic curves and related areas. It is held at Department of Mathematics, Faculty of Science University of Zagreb, Bijenička cesta 30, from September 18 to September 22, 2023.

The scientific program of this workshop consists of invited and contributed talks of international and experts on the subjects covered by the conference.

The index of all authors is given at the end of the brochure.

Supported by

QuantiXLie Center of Excellence, project KK.01.1.1.01.0004
Department of Mathematics, Faculty of Science, University of Zagreb
Zaklada HAZU

Organizing Committee

Filip Najman - chairman, University of Zagreb
Andrej Dujella, University of Zagreb
Matija Kazalicki, University of Zagreb

Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri

Projekt KK.01.1.1.01.0004

Projekt je sufinancirala Europska unija iz Europskog fonda za regionalni razvoj. Sadržaj ovog seminara isključiva je odgovornost Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu te ne predstavlja nužno stajalište Europske unije.

Europska unija
Zajedno do fondova EU

EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI

Operativni program KONKURENTNOST I KOHEZIJA

EUROPSKA UNIJA
Europski fond za regionalni razvoj

Participants

Bryan Advocaat, *University of Luxembourg*
Nikola Adžaga, *University of Zagreb*
Alen Andrašek, *University of Zagreb*
Barinder S. Banwait, *Boston University*
Abbey Bourdon, *Wake Forest University*
Peter Bruin, *Leiden University*
Pete Clark, *University of Georgia, Athens*
Mar Curco Iranzo, *Utrecht University*
Maarten Derickx, *Leiden University*
Andrej Dujella, *University of Zagreb*
Ahmad El-Guindy, *Cairo University*
Lorenzo Furio, *Univeristy of Pisa*
Stevan Gajović, *Charles University Prague*
Andrea Galelse, *Scuola Normale Superiore, Pisa*
Franco Golfieri, *University of Aveiro*
Pip Goodman, *Bayreuth University*
Shin Hattori, *Tokyo City University*
Giacomo Hermes Ferraro, *Sapienza Università di Roma*
Daeyeol Jeon, *Kongju National University*
Yasemin Kara, *Boğaziçi University*
Jaskaran Kaur, *Simon Fraser University*
Timo Keller, *Groningen University*
Matija Kazalicki, *University of Zagreb*
Iva Kodrnja, *University of Zagreb*
Annie Littler, *Boston University*
Elvira Lupoian, *University of Warwick*
Luca Mauri, *Scuola Superiore Universitaria di Toppo Wasserman*
Pietro Mercuri, *Sapienza Università di Roma*
Travis Morrison, *Virginia Tech*
Goran Muić, *University of Zagreb*
Steffen Müller, *University of Groningen*
Filip Najman, *University of Zagreb*
Ivan Novak, *University of Zagreb*
Lukas Novak, *University of Zagreb*
Maryam Nowroozi, *University of Warwick*
Ekin Özman, *Boğaziçi University*
Petar Orlić, *University of Zagreb*
Oana Padurariu, *Max Planck Institute for Mathematics, Bonn*
Antigona Pajaziti, *University of Luxembourg*
Tomislav Pejković, *University of Zagreb*

Antonella Perucca, *University of Luxembourg*
David Roe, *MIT*
Francesco Pappalardi, *Università degli Studi di Roma Tre*
Vinko Petričević, *University of Osijek*
Jeremy Rouse, *Wake Forest University*
Ignasi Sánchez, *Universidad de Barcelona*
Katerina Santicola, *Warwick University*
René Schoof, *Tor Vergata, Rome*
Himanshu Shukla, *University of Bayreuth*
Ivan Soldo, *University of Osijek*
Jim Stankewicz, *IDA*
Peter Stevenhagen, *Leiden University*
Valerio Talamanca, *Roma Tre University*
Kenji Terao, *Warwick University*
Antonela Trbović, *Croatia Osiguranje*
George Ţurcaş, *Babeș-Bolyai University*
Robin Visser, *University of Warwick*
Hwajong Yoo, *Seoul National University*
Benjamin York, *University of Connecticut*
Sonja Žunar, *University of Zagreb*

Zagreb, Croatia, September 18 – 22, 2023
Modular curves and Galois representations

Program

The conference is held at Department of Mathematics, University of Zagreb, Bijenička cesta 30. All talks take place in room A002 on the ground floor.

Monday, September 18, 2023

	Morning session
8:30 - 8:55	Registration
8:55 - 9:00	Opening and Announcements
9:00 - 9:50	*Finite flat group schemes over $\mathbb{Z}$ and GRH* René Schoof
10:00 - 10:25	*Automorphism group of Cartan modular curves* Pietro Mercuri
10:25 - 10:55	coffee break
10:55 - 11:45	*Primitive points on elliptic curves* Peter Stevenhagen
11:55 - 12:20	*Serre's Uniformity Question and proper subgroups of $C_{ns}^{+}(p)$* Lorenzo Furio
12:20 - 14:00	lunch break
	Afternoon session
14:00 - 14:50	*Unified treatment of Artin-type problems* Antonella Perucca
15:00 - 15:25	*Rational Cuspidal Points on the Modular Jacobians $J_H(p)$* Elvira Lupoian
15:25 - 15:50	coffee break
15:50 - 16:40	*Counting rational points on modular curves of genus 0 over number fields* Peter Bruin
16:50 - 17:15	*Anticyclotomic Iwasawa theory and the Birch–Swinnerton-Dyer conjecture for analytic rank 1 at Eisenstein primes of good and bad multiplicative reduction* Timo Keller

Zagreb, Croatia, September 18 – 22, 2023
Modular curves and Galois representations

Tuesday, September 19, 2023

	Morning session
9:00 - 9:50	*p-adic Arakelov theory and quadratic Chabauty* Steffen Müller
10:00 - 10:25	*Computing p-adic heights on hyperelliptic curves* Stevan Gajović
10:25 - 10:50	coffee break
10:50 - 11:40	*Finding low degree places on $X_1(N)$* Mark van Hoeij
11:50 - 12:15	*On the p-isogenies of elliptic curves with multiplicative reduction over quadratic fields* George Ţurcaş
12:15 - 14:00	lunch break
	Afternoon session
14:00 - 14:50	*An Algorithm for Isolated j-invariants* Abbey Bourdon
15:00 - 15:25	*Restrictions on endomorphism algebras* Pip Goodman
15:25 - 15:55	coffee break
15:55 - 17:00	*Lightning talks*

Lightning talks:

1. Ahmad El-Guindy: *Some p-adic properties of modular forms with Nebentypus and p-regular partitions*
2. Franco Golfieri: *About the equation $x^4 + dy^2 = z^p$*
3. Ignasi Sanchez: *An effective algorithm for comparing residually reducible 2-adic Galois representations*
4. Katerina Santicola: *A converse of Faltings' Theorem*
5. Ivan Soldo: *$D(-1)$-quadruples extending certain pairs in imaginary quadratic rings*
6. Kenji Terao: *Maps between isolated points on modular curves*
7. Robin Visser: *Abelian surfaces with good reduction away from 2*

Zagreb, Croatia, September 18 – 22, 2023
Modular curves and Galois representations

Wednesday 20, 2023

	Morning session
9:00 - 9:50	*Modular curves with infinitely many points of degree* 3 *or* 4 Daeyeol Jeon
10:00 - 10:50	*Hyperelliptic and Trigonal modular curves in positive characteristic* Maarten Derickx
10:50 - 11:20	coffee break
11:20 - 12:10	*Determining biellipticity for quotient modular curves* Francesc Bars
12:20 - 12:45	*Modular curves* $X_0(N)$ *with infinitely many points of degree* d Petar Orlić
	Free afternoon

Zagreb, Croatia, September 18 – 22, 2023
Modular curves and Galois representations

Thursday, September 21, 2023

	Morning session
9:00 - 9:50	*Local-global trace relations and their implications* Ekin Özman
10:00 - 10:25	*Low degree points on modular curves and their quotients* Nikola Adžaga
10:25 - 10:55	coffee break
10:55 - 11:45	*Torsion groups of elliptic curves over quadratic fields* $\mathbb{Q}(\sqrt{d})$ *for* $\lvert d\rvert < 500$ Barinder Banwait
11:55 - 12:20	*Rational points on Atkin-Lehner quotients of geometrically hyperelliptic Shimura curves* Oana Padurariu
12:20 - 14:00	lunch break
	Afternoon session
14:00 - 14:50	*Report on the CM case: torsion points, Galois representations and modular curves* Pete Clark
14:50 - 15:20	coffee break
15:20 - 16:10	*Modular Curves in the LMFDB* David Roe
19:30	Conference dinner

Zagreb, Croatia, September 18 – 22, 2023
Modular curves and Galois representations

Friday, September 22, 2023

	Morning session
9:15 - 10:05	*The rational torsion subgroup of $J_0(N)$* Hwajong Yoo
10:15 - 11:05	*Hilbert's Irreducibility, Modular Forms, and Computation of Certain Galois Groups* Goran Muić
11:05 - 11:35	coffee break
11:35 - 12:25	*Minimal images of Galois for elliptic curves* Jeremy Rouse
	End of Conference

Abstracts of talks

Low degree points on modular curves and their quotients

Nikola Adžaga
University of Zagreb

We discuss low-degree points on modular curves $X_0(N)$ and $X_1(N)$, as well as the quotients of $X_0(N)$ by Atkin-Lehner involutions. These curves serve as moduli spaces for elliptic curves with additional structures.

We employ variations of Chabauty's method, such as the quadratic Chabauty, to provably determine all $\mathbb{Q}$-rational points on curves $X_0^+(p)$ of genus up to 6 (for prime p). We also classify $\mathbb{Q}$-rational points on such $X_0^+(p)$ and on hyperelliptic $X_0^*(N)$ when N is squarefree.

We introduce enhancements to the symmetric Chabauty method, enabling us to determine all the quadratic points on $X_0(N)$ for numerous levels N. We also apply techniques such as the Mordell-Weil Sieve and use quotients to elliptic curves, etc.

This presentation encompasses several works, including some of speaker's written jointly with many coauthors (Arul, Beneish, Chen, Chidambaram, Keller, Michaud-Jacobs, Najman, Ozman, Padurariu, Vukorepa and Wen), as well as a selection of both classical and recent results.

Torsion groups of elliptic curves over quadratic fields $\mathbb{Q}(\sqrt{d})$ for $|d| < 500$

Barinder S. Banwait
Boston University

We study the problem of determining the groups that can arise as the torsion subgroup of an elliptic curve over a fixed quadratic field, building on work of Kamienny-Najman, Krumm, and Trbović. By employing techniques to study rational points on curves developed by Bruin and Stoll, we are able to determine the possible torsion subgroups of elliptic curves over quadratic fields $\mathbb{Q}(\sqrt{d})$ for all squarefree d with $|d| < 500$. This is a joint work in progress with Maarten Derickx.

Determining biellipticity for quotient modular curves

Francesc Bars
UAB Barcelona

Let C be a non-singular projective curve defined over a number field K with genus ≥ 2. By a result of Faltings, the L-points of the curve, $C(L)$, is a finite set, where L is a finite field extension of K. Assume that C is not-hyperelliptic curve. If C has a degree two map to an elliptic curve E (i.e. C is bielliptic) then the set of quadratic points $\Gamma_2(C, M) = \cup_{[L:M]\leq 2} C(L)$ is infinite for some number field M, and Silverman-Harris observed that the converse is true (such infinitenes of the set $\Gamma_2(C, M)$ for certain number field M will occurs iff C is bielliptic or hyperelliptic). Moreover there are more arithmetical results in fixing the field M where such phenomena occurs (see more details in [2]).

Modular curves are moduli spaces classifying elliptic curves with certain level structure, and determine its L-points always has key interest.

The main part of the talk we will discuss the main ideas in order to obtain the list of the quotient modular curves, (i.e. $X_0(N)/W_N$ with W_N a subgroup of the group $B(N)$ generated by all Atkin-Lehner involutions associated with $X_0(N)$) which are bielliptic (works appeared in [1], [9], [4],[5],[7],[8]).

If the time permits, by using previous ideas on involutions and the results in [6] we will observe results on automorphisms group for quotient modular curves for square free levels [3] (joint work with T. Dalal).

References

[1] F. Bars: Bielliptic modular curves. J. Number Theory 76 (1999), no. 1, 154–165.

[2] F. Bars: On quadratic points of classical modular curves. Contemporary Mathematics, Momose memorial Volume, Vol. 701, 17–34, (2018).

[3] F. Bars, T. Dalal: Automorphism group of quotient curves $X_0(pq)$. Preprint, August 2023.

[4] F.Bars, J. González Rovira: Bielliptic modular curves $X_0^*(N)$ with square-free levels. Mathematics of Computation 88 (320), 2939–2957 (2019).

[5] F.Bars, J. González Rovira: Bielliptic modular curves $X_0^*(N)$. Journal of Algebra 559, 726-759, (2020).

[6] F. Bars, J. González Rovira: The automorphism group of the modular curve $X_0^*(N)$ with square-free levels. Trans. Amer. Math. Soc. 374 (2021), 5783–5803.

[7] F.Bars, J. González Rovira, M. Kamel: Bielliptic quotient modular curves with N square-free. Journal of Number Theory 216, 380-402, (2020).

[8] F.Bars, M.Kamel, A. Schweizer: Bielliptic quotient modular curves. Mathematics of Computation AMS Volume 92, Number 340, (2023), Pages 895–929.

[9] D. Jeon: Bielliptic modular curves $X_0^+(N)$. Journal of Number Theory 185, (2018), 319–338.

An Algorithm for Isolated j-invariants

Abbey Bourdon

Wake Forest University

In this talk, I will discuss a new algorithm which can be used to determine whether an elliptic curve with rational j-invariant gives rise to an isolated point on some modular curve $X_1(n)$. Our results are most compelling in the case of $\mathbb{P}^1$-isolated points, which are those not induced by a rational map to the projective line of the same degree. Running the algorithm on all elliptic curves presently in the LMFDB gives evidence for the conjecture that $j \in \mathbb{Q}$ is the image of a $\mathbb{P}^1$-isolated point if and only if j corresponds to an elliptic curve with complex multiplication or $j = -140625/8, -9317, 351/4$, or -162677523113838677.

This is joint work with Sachi Hashimoto, Timo Keller, Zev Klagsbrun, David Lowry-Duda, Travis Morrison, Filip Najman, and Himanshu Shukla.

Counting rational points on modular curves of genus 0 over number fields

Peter Bruin

Leiden University

This talk is about the problem of counting rational points of bounded height on (stacky) modular curves whose coarse moduli space has genus 0. First, we will survey various older and newer definitions of height functions on stacks, with a focus on weighted projective stacks. Next, we will give an overview of recent results on counting points with respect to such height functions. Finally, we will give applications to counting elliptic curves with prescribed level structure over number fields. This is partly based on joint work with Filip Najman and with Irati Manterola Ayala.

Report on the CM case: torsion points, Galois representations and modular curves

Pete Clark

University of Georgia, Athens

This talk will be a survey of work done on torsion points and Galois representations for elliptic curves over number field with complex multiplication (CM). (You will not be shocked to hear that modular curves also come into the picture.) Although many results will be mentioned, I will spend the most time on my recent work with F. Saia that gives a complete classification of torsion subgroups of CM elliptic curves over number fields of any fixed degree (with some fine print to be discussed). After all this one can ask; what remains to be done in the CM case? I will end by mentioning some open problems, both for CM elliptic curves and for CM abelian varieties.

Hyperelliptic and trigonal modular curves in positive characteristic

Maarten Derickx

Leiden University

In this joint work with Filip Najman we classify the pairs p, N where N is an integer and p is a prime coprime to N such that the modular curve $X_0(N)$ is hyperelliptic or trigonal over $\mathbb{F}_p$. We also do this classification for the algebraic closure of $\mathbb{F}_p$. This classification is already known for the modular curves $X_0(N)$ over $\mathbb{Q}$ and $\mathbb{C}$. The main reason this classification up to now has only been done over $\mathbb{C}$ and not in positive characteristics, is that the best known lower bounds on the gonalities of modular curves depend on the characteristic, and these bounds get significantly worse once the characteristic is large with respect to the level. Filip and I circumvent these problems by using a geometric argument that shows that for N large enough the gonality of $X_0(N) > 4$ in a way that is independent of the characteristic. We conjecture that more generally it should be possible to bound the gonality of $X_0(N)$ from below in a way that is independent of the characteristic. Additionally we show that for non hyperelliptic $X_0(N)$ of genus 4 the $\mathbb{F}_p$ gonality of $X_0(N)$ is linked to the splitting behavior of p in a quadratic number field depending on N.

Serre's Uniformity Question and proper subgroups of $C_{ns}^{+}(p)$

Lorenzo Furio

Univeristy of Pisa

In 1972 Serre proved his celebrated Open Image Theorem, stating that for every rational elliptic curve E without complex multiplication there exists an integer N_E such that, for every prime $p > N_E$, the Galois representation $\rho_{E,p}$ is surjective onto $\mathrm{GL}_2(\mathbb{F}_p)$. In the same article, he asked whether the constant N_E can be taken to be independent of the curve, and this became known as Serre's Uniformity Question. In this talk, I will discuss the current progress towards an answer to this question, in particular the Runge method for modular curves developed by Bilu and Parent and the recent improvements obtained via this method by Le Fourn and Lemos, as well as explain how to solve some of the questions left open by the latter result.

This is joint work with Davide Lombardo.

Computing p-adic heights on hyperelliptic curves

Stevan Gajović

Charles University Prague

In this talk, we present an algorithm to compute p-adic heights on hyperelliptic curves with good reduction. Our algorithm improves a previous algorithm of Balakrishnan and Besser by being considerably simpler and faster and allowing even degree models. We discuss two applications of our work to modular curves: to the quadratic Chabauty method and to numerically test the p-adic Birch and Swinnerton-Dyer conjecture in examples. This is joint work with Steffen Müller.

Restrictions on endomorphism algebras

Pip Goodman
Bayreuth University

Given a hyperelliptic curve $y^2 = f(x)$ defined over a number field, can one find simple conditions on f to determine whether its Jacobian is absolutely simple or not? Or, even better, obtain information on the structure of its (geometric) endomorphism ring?

Zarhin has shown that in many cases when the Galois group of f is "large" (insoluble, two-transitive, ...) the possibilities for the endomorphism ring are heavily restricted. In this talk, we will see that many restrictions persist when the Galois group of f is merely cyclic of large prime order. In fact, for certain base fields, we are able to give a finite explicit list.

Finding low degree places on $X_1(N)$

Mark van Hoeij
Florida State University

A low degree place is a non-cuspidal place on $X_1(N)$ whose degree is less than the (conjectured, if $N > 40$) gonality. Explicit examples for $N \leq 80$ are listed at www.math.fsu.edu/ hoeij/files/X1N and their degrees are tabulated in arXiv:1202.4355. In the talk I'll explain the probabilistic approach that was used to find these low degree places, and for which values of N one may be able to prove completeness.

Modular curves with infinitely many points of degree 3 or 4

Daeyeol Jeon
Kongju National University

We are considering the problem of determining which modular curves can have infinitely many rational points over the number fields with fixed degree d over $\mathbb{Q}$. If $d = 1$, we know that only modular curves of genus 0 or 1 can have infinitely many rational points by Faltings. If $d = 2$, we can conclude that a modular curve X over $\mathbb{Q}$ has infinitely many rational points over the quadratic number fields if and only if X admits a $\mathbb{Q}$-rational map to a projective line or an elliptic curve with a positive rank over $\mathbb{Q}$ by the results of Abramovich, Bars, Harris, and Silverman. We would like to think about this problem for $d = 3$ or 4. Also we're also considering the problem of determining which modular curves can allow $\mathbb{Q}$-rational maps of degree $d = 3$ or 4 to elliptic curves.

Anticyclotomic Iwasawa theory and the Birch–Swinnerton-Dyer conjecture for analytic rank 1 at Eisenstein primes of good and bad multiplicative reduction

Timo Keller

University of Groningen

We report on work in progress with Mulun Yin. Castella–Gross–Lee–Skinner recently proved Perrin-Riou's Heegner point main conjecture for modular abelian varieties at odd primes p of good reduction for which the mod-p Galois representation ρ_p is reducible ("Eisenstein primes"). They have the restriction that the characters in the semisimplification of ρ_p are non-trivial on $Gal_{\mathbb{Q}_p}$. For example this excludes the case when there is a non-trivial p-torsion point.

We are working on removing this restriction and generalize the result to newforms of higher weight, allowing us to also treat bad multiplicative reduction using Hida theory. As a consequence, we get the p-part of the Birch–Swinnerton-Dyer conjecture for analytic rank 1 (and 0 by Castella–Grossi–Skinner) and a p-converse theorem.

Combining this with previous results of Kato, Skinner–Urban, Skinner, ..., Castella–Çiperiani–Skinner–Sprung, we get the strong BSD conjecture in analytic rank 0 and 1 for squarefree level N under a mild condition on the discriminant except maybe for the 2-part.

Rational Cuspidal Points on the Modular Jacobians $J_H(p)$

Elvira Lupoian

Warwick University

The rational points of an arbitrary modular curve are often studied by looking at their image in the Jacobian, under the Abel-Jacobi embedding. Although it's often the non-cuspidal points that are of interest, studying the cuspidal points is often accessible and more effective than one might first think.

The theorem of Manin and Drinfeld tell us that the difference of two cusps is a torsion point on the Jacobian of a modular curve, and hence we can consider the finite subgroup generated by the cusps in the Jacobian. On the classical modular curve $X_0(p)$ of prime level $p \geq 5$, there are two cusps, both defined over $\mathbb{Q}$, and Ogg proved that their difference generates a cyclic subgroup of order the numerator of $\frac{p-1}{12}$. Mazur later proved that this subgroup is in fact the entire rational torsion subgroup of the Jacobian $J_0(p)$. This phenomenon is expected to be more general. In this talk, we will consider the intermediate

modular curve $X_H(p)$, where H is a proper subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ and describe some cuspidal subgroups corresponding to these curves.

Automorphism group of Cartan modular curves

Pietro Mercuri

Sapienza Università di Roma

We consider the modular curves associated to a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ or to a particular class of subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ containing the Cartan subgroup as a normal subgroup. We describe the automorphism group of these curves when the level is large enough. If time permits, we give a sketch of the proof.

Hilbert's Irreducibility, Modular Forms, and Computation of Certain Galois Groups

Goran Muić

University of Zagreb

We consider the modular curves associated to a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ or to a particular class of subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ containing the Cartan subgroup as a normal subgroup. We describe the automorphism group of these curves when the level is large enough. If time permits, we give a sketch of the proof.

In this talk we discuss applications of our earlier works [1] and [2] in studying certain Galois groups and splitting fields of rational functions in $\mathbb{Q}(X_0(N))$ using Hilbert's irreducibility theorem and modular forms (see [3]). We also consider computational aspect of the problem using MAGMA and SAGE.

This is joint work with Iva Kodrnja.

References

[1] G. Muić, *On degrees and birationality of the maps $X_0(N) \to \mathbb{P}^2$ constructed via modular forms,* Monatsh. Math. **Vol. 180, No. 3**, 607–629, (2016).

[2] G. Muić, I. Kodrnja *On primitive elements of algebraic function fields and models of $X_0(N)$,* The Ramanujan Journal, **55** No. 2,(2021).

[3] G. Muić, I. Kodrnja *Hilbert's irreducibility, modular forms, and computation of certain Galois groups,* J. Number Theory **253**, 114–136 (2023).

---

p-adic Arakelov theory and quadratic Chabauty

Steffen Müller

Groningen University

The quadratic Chabauty method for the computation of rational points on certain curves, due to Balakrishnan and Dogra, is the simplest nontrivial instance of Kim's nonabelian Chabauty. Based on p-adic Hodge theory, it produces a p-adic function F and a finite set T such that F maps the rational points into T. While T can be shown to be trivial for several interesting modular curves, its computation is in general a difficult problem. I will present an alternative approach to quadratic Chabauty that is based on p-adic Arakelov theory. I will also discuss work in progress that uses this idea to obtain an algorithm to compute the set T. This is joint work with Amnon Besser and Padmavathi Srinivasan.

Modular curves $X_0(N)$ with infinitely many points of degree d

Petar Orlić

University of Zagreba

We present a method of finding all possible degrees of rational morphisms from $X_0(N)$ to a fixed elliptic curve. We can use this result to determine all curves $X_0(N)$ with infinitely many quartic points.

Rational points on Atkin-Lehner quotients of geometrically hyperelliptic Shimura curves

Oana Padurariu

Max Planck Institute for Mathematics, Bonn

Guo and Yang gave defining equations for all geometrically hyperelliptic Shimura curves $X_0(D, N)$. In this talk, I will describe how we created a database containing all their Atkin-Lehner quotients and how we computed their sets of $\mathbb{Q}$-rational points when these sets are finite. We also determine which rational points are CM for many of these curves. This is joint work with Ciaran Schembri.

Local-global trace relations and their implications

Ekin Özman

Boğaziçi University

Let E be an elliptic curve defined over the rational numbers and K be a quadratic number field. In this talk we will explore the necessary and sufficient conditions for local-global trace obstructions of the trace map from $E(K)$ to $E(\mathbb{Q})$. Then we will mention some statistical results and heuristics implied by these observations. This is joint work with Mirela Çiperiani.

Unified treatment of Artin-type problems

Antonella Perucca

University of Luxembourg

Since Hooley's seminal 1967 resolution of Artin's primitive root conjecture under the Generalized Riemann Hypothesis, numerous variations of the conjecture have been considered. We present a framework generalizing and unifying many previously considered variants, and prove results in this full generality (under GRH). This is joint work with Olli Järviniemi and Pietro Sgobba.

Modular Curves in the LMFDB

David Roe

Massachusetts Institute of Technology

I will describe the methods used to create the database of modular curves that has been added to the LMFDB this summer, which can be divided into several stages. The first stage involves computing the lattice of subgroups of $\mathrm{GL}(2, N)$ up to conjugacy, or at least those with surjective determinant (corresponding to modular curves defined over $\mathbb{Q}$). The second involves decomposing the Jacobian into modular abelian varieties associated to newforms. The third stage is finding models using various methods, and the fourth is producing rational points by computing Galois images for elliptic curves in the LMFDB elliptic curve databases. I will finish by explaining the next steps for this database, as well as the obstacles that stand in our way.

Minimal images of Galois for elliptic curves

Jeremy Rouse

Wake Forest University

Let S be a finite set of primes. We say that a finite index $H \subseteq \mathrm{GL}_2(\mathbb{Z}_S)$ is a minimal subgroup if $\det : H \to \mathbb{Z}_S^\times$ is surjective, but for every proper closed subgroup $K \subseteq H$, $\det : K \to \mathbb{Z}_S^\times$ is not surjective.

Any non-CM elliptic curve $E/\mathbb{Q}$ with bad reduction only at 2 has the property that $\operatorname{im} \rho_{E,2^\infty}$ is a minimal subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$. We show that minimal subgroups only exist in the case that $S = \{2\}$. Moreover, for any finite index subgroup $H \subseteq \mathrm{GL}_2(\mathbb{Z}_2)$, there is finite index $L \subseteq H$ that is minimal. We compute models of all genus zero modular curves X_H for minimal $H \subseteq \mathrm{GL}_2(\mathbb{Z}_2)$, and give an infinite set of elliptic curves over imaginary quadratic fields with bad reduction only at 2 with minimal 2-adic image.

Finite flat group schemes over $\mathbb{Z}$ and GRH

René Schoof
University of Rome Tor Vergata

Since simple commutative finite flat group schemes G over $\mathbb{Z}$ are killed by a prime number p, their order is a power of p. Tate asked whether a simple group scheme G is necessarily equal to $\mathbb{Z}/p\mathbb{Z}$ or μ_p. This has been proved for primes $p \leq 19$. Under assumption of the Generalized Riemann Hypothesis we extend this result to primes $p \leq 37$. This is joint work with Lassina Dembele.

Primitive points on elliptic curves

Peter Stevenhagen
Leiden University

Given a point P of infinite order on an elliptic curve E defined over a number field K, one may ask, after Lang and Trotter, whether the set of primes $\mathfrak{p}$ of K for which the reduction of P generates the point group over the residue class field of $\mathfrak{p}$ possesses a density. There is a heuristical density that has not been proven to be correct, not even under GRH. We will focus on the vanishing of the heuristical density. This is a question which may be answered without GRH, and which has more subtleties than the analogous question for the more classical multiplicative case of Artin's conjecture on primitive roots. This is joint work with Francesco Pappalardi (Rome) and Nathan Jones (Chicago).

On the p-isogenies of elliptic curves with multiplicative reduction over quadratic fields

George Ţurcaş
Babeş-Bolyai University

Throught this talk, we will present some sufficient conditions that demonstrate certain infinite families of elliptic curves defined over a fixed quadratic field K do not have p-isogenies, for primes p larger than a constant B_K. We will also comment on some examples of elliptic curves with p-isogenies for large primes p, corresponding to quadratic points on bielliptic modular curves which were found computationally.

The rational torsion subgroup of $J_0(N)$

Hwajong Yoo
Seoul National University

In this talk, we discuss some recent progress in the work of generalized Ogg's conjecture which asserts that the rational torsion subgroup of $J_0(N)$ is equal to the rational cuspidal subgroup of $J_0(N)$. If time permits, we introduce some idea to compute the rational cuspidal subgroup of $J_0(N)$.

On the adelic image of Galois representations attached to elliptic curves with CM

Benjamin York
University of Connecticut

Let E be an elliptic curve defined over a number field K, and let ρ_E be the adelic Galois representation attached to E/K. In this talk, we will discuss a method for computing adelic images of elliptic curves over $\mathbb{Q}$ with complex multiplication. This work is joint with Álvaro Lozano-Robledo

---

Index