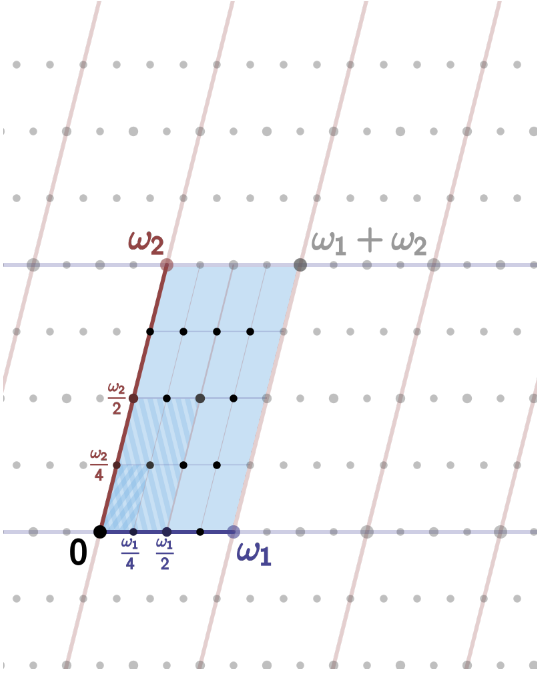
QuantiXLie Center of Excellece
&
Department of Mathematics, Faculty of Science,
University of Zagreb

Book of Abstracts

Torsion groups and Galois representations of elliptic curves



June 25 – 29, 2018, Zagreb, Croatia

Preface

This brochure consists of the program of presentations and abstracts of papers presented at the *Torsion groups 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 torsion groups 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 June 25 to June 29, 2018.

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

Samuele Anni, *MPIM Bonn*
Nikola Adžaga, *University of Zagreb*
Razvan Barbalescu, *Institut de Mathématiques de Jussieu Paris Rive Gauche*
Daniel Berhanu, *University of Luxembourg*
Marija Bliznac-Trebješanin, *University of Split*
Abbey Bourdon, *Wake Forest*
Peter Bruin, *Leiden University*
Victoria Cantoral-Farfan, *ICTP Trieste*
Michael Chou, *Tufts University*
Nirvana Copolla, *Bristol University*
Harris Daniels, *Amherst College*
Mahadi Ddamulira, *TU Graz*
Maarten Derickx, *MIT*
Vladimir Dokchitser, *King's College London*
Andrej Dujella, *University of Zagreb*
Tom Fisher, *Cambridge University*
Linda Frey, *University of Basel*
Jedrzej Garnek, *Adam Mickiewicz University, Poznan*
Enrique Gonzalez-Jimenez, *UAM Madrid*
Pip Goodman, *Bristol University*
Tomislav Gužvić, *University of Zagreb*
Parham Hamidi, *University of Waterloo*
Bernadin Ibrahimpašić, *University of Bihać*
Borka Jadrijević, *University of Split*
Sameerah Jamal, *University of the Witwatersrand, Johannesburg*
Daeyeol Jeon, *Kongju National University*
Abhishek Juyal, *Motilal Nehru National Institute of Technology, Allahabad*
Aleksandra Kaim, *Adam Mickiewicz University, Poznan*
Matija Kazalicki, *University of Zagreb*
Dijana Kreso, *University of British Columbia*
Ivan Krijan, *University of Zagreb*
Jun Ho, *Lee Mokpo National University*
Pedro Lemos, *MPIM, Bonn*
Alvaro Lozano-Robledo, *University of Connecticut*
Loïc Merel, *Institut de Mathématiques de Jussieu Paris Rive Gauche, Université Paris Diderot*
Damir Mikoč, *University of Zadar*
Filip Najman, *University of Zagreb*
Kazuta Ota, *Keio University*
Lorenzo Pagani, *Sapienza University Rome*

Pïerre Parent, *University of Bordeaux*
Antonella Perucca, *University of Luxembourg*
Vinko Petričević, *University of Zagreb*
Marusia Rebolledo, *Université Blaise Pascal Clermont Ferrand*
Jeremy Rouse, *Wake Forest University*
Rene Schoof, *Tor Vergata, Rome*
Devika Sharma, *Weizmann Institute*
Sudarshan Shinde, *Institut de Mathématiques de Jussieu Paris Rive Gauche*
Peter Stevenhagen, *Leiden University*
Michael Stoll, *University of Bayreuth*
Andrew Sutherland, *MIT*
Emiliano Torti, *University of Luxembourg*
Antonela Trbović, *University of Zagreb*
George Turcas, *University of Warwick*
Andrei Yafaev, *University College London*
Jeff Yelton, *University of Milan*
David Zureick-Brown, *Emory University*

Program

The conference is held at Department of Mathematics, University of Zagreb, Bijenička cesta 30. All talks take place in room A101 on the first floor.

Monday, June 25, 2018

	Morning session
8:45 - 9:15	Registration
9:15 - 9:30	Opening and Announcements
9:30 - 10:20	*Current methods versus expectations in the asymptotic of uniform boundedness* Loïc Merel
10:30 - 10:55	*On Fermat's equation over some quadratic imaginary number fields* George Turcas
11:20 - 11:45	coffee break
11:15 - 12:05	*On families of* n*-congruent elliptic curves* Tom Fisher
12:05 - 14:00	lunch break
	Afternoon session
14:00 - 14:50	*Stable models for modular curves in prime level* Pïerre Parent
15:00 - 15:25	*Reductions of points on elliptic curves* Antonella Perucca
15:25 - 15:45	coffee break
15:45 - 16:35	*Torsion points of an elliptic curve over* $\mathbb{Q}(\sqrt{37})$ Rene Schoof
16:45 - 17:10	*Local torsion of elliptic curves* Jędrzej Garnek

Tuesday, June 26, 2018

	Morning session
9:00 - 9:50	*Progress on Mazur's program B, part I : an overview* Maarten Derickx
10:00 - 10:25	*Progress on Mazur's program B, part II: equations of modular curves* Jeremy Rouse
10:25 - 10:45	coffee break
10:45 - 11:35	*Progress on Mazur's program B, part III: rational points* David Zureick-Brown
11:45 - 12:10	*Some cases of Serre's uniformity problem* Pedro Lemos
12:10 - 14:00	lunch break
	Afternoon session
14:00 - 14:50	*Primitivity of points on elliptic curves* Peter Stevenhagen
15:00 - 15:25	*Torsion of CM elliptic curves defined over the maximal abelian extension of $\mathbb{Q}$* Michael Chou
15:25 - 15:45	coffee break
15:45 - 16:35	*A classification of p-adic Galois representations attached to elliptic curves with CM* Álvaro Lozano-Robledo
16:45 - 17:10	*Groups of generalized G-type and applications to torsion subgroups of rational elliptic curves over infinite extensions of $\mathbb{Q}$* Harris Daniels

Wednesday, June 27, 2018

	Morning session
9:00 - 9:50	*Sporadic Points with j-invariant of Bounded Degree* Abbey Bourdon
10:00 - 10:50	*Automorphism groups of modular curves and torsion subgroups of elliptic curves* Daeyeol Jeon
10:50 - 11:15	coffee break
11:15 - 12:05	*A moduli interpretation for the non split Cartan modular curves: necklaces* Marusia Rebolledo
	Free afternoon

Thursday, June 28, 2018

	Morning session
9:00 - 9:50	*Counting points on modular curves* Andrew Sutherland
10:00 - 10:25	*A cryptographic application of modular curves* Razvan Barbulescu
10:25 - 10:45	coffee break
10:45 - 11:35	*Growth of torsion groups of elliptic curves upon base change: a computational approach* Enrique González-Jiménez
11:45 - 12:10	*Torsion groups of elliptic curves over quadratic fields* $\mathbb{Q}(\sqrt{d}),\ 0 < d < 100$ Antonela Trbović
12:10 - 14:00	lunch break
	Afternoon session
14:00 - 14:50	*Bad reduction on hyperelliptic curves* Vladimir Dokchitser
15:00 - 15:25	*Prime-to-p actions of inertia associated to semistable hyperelliptic curves* Jeff Yelton
15:25 - 15:45	coffee break
15:45 - 16:10	*New cases of the Mumford-Tate conjecture for abelian varieties* Victoria Cantoral-Farfán
16:20 - 16:45	*Explicit Small Height Bound for* $\mathbb{Q}(E_{tor})$ Linda Frey
16:55 - 17:20	*Semistable elliptic curves over totally real fields* Samuele Anni
19:30	Confernce dinner

Friday, June 29, 2018

	Morning session
9:00 - 9:50	*Simultaneous torsion in the Legendre family of elliptic curves* Michael Stoll
10:00 - 10:50	*TBA* Pete Clark
10:50 - 11:15	coffee break
11:15 - 12:05	*Towards a database of Galois representations* Peter Bruin
	End of conference

Abstracts of talks

Semistable elliptic curves over totally real fields

Samuele Anni

Max Planck Institute for Mathematics, Bonn

In this talk, I will present a bound for the degree of isogenies between semistable elliptic curves over totally real fields. This bound is particularly helpful for studying Diophantine equations. Moreover, I will show some results about elliptic curves with prime conductor over totally real fields and their isogeny classes.

A cryptographic application of modular curves

Razvan Barbulescu and Sudarshan Shinde

Institut de Mathématiques de Jussieu Paris Rive Gauche

The elliptic curve method (ECM) is an algorithm to find all the factors less than a bound B of an integer N when B is much smaller than N. It is used as a building block in the number field sieve (NFS), where a non-negligible fraction of time is spent for finding the primes less than an integer B in the norms of a large number of algebraic integers in a fixed number field.

In a classical variant, when given an integer N which has a prime factor $p < B$, ECM consists in enumerating elliptic curves E defined over $\mathbb{Q}$ and doing a fast computation which succeeds in finding p if $\#E(\mathbb{F}_p)$ is B_1-smooth, i.e. all its prime factors are less than a bound B_1, which is fixed and can be different than B. As the number of curves needed is not bounded, it is necessary to use infinite families of elliptic curves, in particular when they are described by modular curves they must have genus zero or one.

Since ECM is used on a large set of integers N, it is unanimously accepted that ECM is sped-up when using families of elliptic curves such that $\#E(\mathbb{F}_p)$ is B_1-smooth for a large proportion of primes p. In a practical approach, Montgomery used the average value of $\mathrm{val}_\ell \#E(\mathbb{F}_p)$ when p varies to compare different families of curves, method for which we propose a new of view.

Barbulescu et al. proved that the average value of $\mathrm{val}_\ell \#E(\mathbb{F}_p)$ for a fixed elliptic curve E is determined by the image of the Galois group of field generated by the coordinates of the ℓ-adic Tate module. Hence, searching for ECM-friendly curves boils down to classifying the elliptic curves whose Galois image is contained in each subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$.

In two contemporanous papers, Rouse and Zureick-Brown, and Sutherland and Zywina classified the possible images of the Galois group in $\mathrm{GL}_2(\mathbb{Z}_2)$ and respectively $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for those subgroups H which contain $-I$. We continued their classification for the subgroups H of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ of genus zero and one not containing $-I$.

In a recent variant of NFS, one applies ECM to integers N such that a fixed polynomial h has an explicit root modulo N. For example, in a recent record computation half of the input integers were of the form $a^4 + b^4$ with a and b integers in a rectangle, where the polynomial Φ_8 has the explicit root a/b. ECM can be easily modified to use elliptic curves defined over $\mathbb{Q}(\zeta_8)$ where there exist families with Galois group in subgroups which are not obtained by the curves defined over $\mathbb{Q}$. This is a new application for several works in the literature.

Towards a database of Galois representations

Peter Bruin

University of Leiden

I will explain a compact way of encoding representations of the absolute Galois group of a field K on finite Abelian groups. This is done via *dual pairs of finite K-algebras*; these are in principle equivalent to finite commutative group schemes or Hopf algebras, but are easier to compute and to store. I will show how to compute these objects and to work with them, with examples coming from torsion subschemes of elliptic curves and from modular forms over finite fields. Work is ongoing to include such representations in the L-Functions and Modular Forms Database.

Sporadic Points with j-invariant of Bounded Degree

Abbey Bourdon

Wake Forest University

Our work is motivated by the following classification problem: For a fixed positive integer d, what finite groups arise as the torsion subgroup of an elliptic curve defined over a number field of degree d? A serious challenge in attempting to extend the classification beyond $d = 1$ or $d = 2$ is the need to identify all groups which arise for only finitely many isomorphism classes of elliptic curves. The known examples correspond to elliptic curves with a rational point of order N appearing in unusually low degree; that is, they correspond to sporadic points on the modular curve $X_1(N)$. In this talk, I will discuss recent results concerning sporadic points of $X_1(N)$ which arise from elliptic curves with j-invariant in an extension of bounded degree. This is joint work with Ozlem Ejder, Yuan Liu, Frances Odumodu, and Bianca Viray.

New cases of the Mumford-Tate conjecture for abelian varieties

Victoria Cantoral-Farfán

ICTP, Trieste

Building on work of Serre, Pink, Banaszak, Gajda and Krasón, we prove the Mumford–Tate conjecture for a few new cases of abelian varieties fully of Lefschetz type. Moreover we will discuss some further applications in the direction of the algebraic Sato–Tate conjecture.

Torsion of CM elliptic curves defined over the maximal abelian extension of $\mathbb{Q}$

Michael Chou

Tufts University

The first main theorem of complex multiplication relates the field of definition of torsion points of a CM elliptic curve in terms of certain ray class fields. In this talk we show how this idea can be used to give a (partial) classification of the torsion structures that can arise for CM elliptic curve defined over the maximal abelian extension of $\mathbb{Q}$. This is joint work with Pete Clark and Marko Milosevic.

TBA

Pete Clark

University of Georgia, Athens

Groups of generalized G-type and applications to torsion subgroups of rational elliptic curves over infinite extensions of $\mathbb{Q}$

Harris Daniels

Amherst College

Recently there has been much interest in studying the torsion subgroups of elliptic curves base-extended to infinite extensions of $\mathbb{Q}$. In this talk we study what happens with the torsion of an elliptic curve E over $\mathbb{Q}$ when changing base to the compositum of all number fields with Galois group G for a fixed group G.We start with a survey of what is known and then continue studying the problem by giving a group theoretic condition called generalized G-type, which is a necessary condition for a number field with Galois group H to be contained in that compositum. In general, group theory allows one to reduce the original problem to the question of finding rational points on finitely many modular curves. To illustrate this method we completely determine which torsion structures occur for elliptic curves defined over $\mathbb{Q}$ and base-changed to the compositum of all fields whose Galois group is of generalized A_4-type.

Progress on Mazur's program B, part I : An overview

Maarten Derickx

University of Groningen

In this talk I will recall many classical results that are known about the possible images of Galois of an elliptic curve over Q. Presenting both classical results like Serre's open image theorem, as well as progress that has since be made in proving that the index of the image of Galois can be bounded independently of the elliptic curve. This involves discussing results on the images of Galois mod p as well as well as the p-adic and adelic version. The main goal is to present the general approach to these questions in a nice and uniform way and laying a firm foundation for later talks by Jeremy Rouse and David Zureick-Brown on recent work in this direction.

Bad reduction on hyperelliptic curves

Vladimir Dokchitser
King's College London

Let $C : y^2 = f(x)$ be a hyperelliptic curve over a local field K of odd residue characteristic. I will explain how to use elementary combinatorial data of the configuration of the roots of $f(x)$ in order to extract many arithmetic invariants of the curve and its Jacobian. I will primarily focus on the Galois representation of the curve, but will also touch on the conductor, minimal discriminant, regular model and the Tamagawa number of the Jacobian. This is joint work with Tim Dokchitser, Celine Maistret and Adam Morgan.

On families of n-congruent elliptic curves

Tom Fisher
Cambridge University

Elliptic curves E and E' are said to be n-congruent if their n-torsion subgroups are isomorphic as Galois modules. The elliptic curves n-congruent to a given elliptic curve are parametrised by (the non-cuspidal points of) certain twists of the modular curve $X(n)$. I will discuss methods for computing equations for these curves, and also for the surfaces that parametrise pairs of n-congruent elliptic curves.

Explicit Small Height Bound for $\mathbb{Q}(E_{\mathbf{tor}})$

Linda Frey
University of Basel

Let E be an elliptic curve defined over $\mathbb{Q}$. We will show that there exists an explicit constant C which is only dependent on the conductor and the $j-$invariant of E such that the absolute logarithmic Weil height of an $\alpha \in \mathbb{Q}(E_{\text{tor}})^* \setminus \mu_\infty$ is always greater than C where E_{tor} denotes all the torsion points of E and μ_∞ are the roots of unity.

Local torsion of elliptic curves

Jędrzej Garnek

Adam Mickiewicz University, Poznan

Let us fix an elliptic curve E defined over the field of rational numbers. If we consider this curve over the field of p-adic numbers and let p vary, the behaviour of the p-torsion of E becomes hard to predict. A conjecture stated by David and Weston in 2008 claims that the p-torsion should "get more complex" as p gets big. It turns out that the conjecture of David and Weston for curves with complex multiplication leads to looking for primes in some recurrence sequences. In the second part of the talk we will discuss lower bounds on the class numbers of the division fields of elliptic curves and abelian varieties.

Growth of torsion groups of elliptic curves upon base change: a computational approach

Enrique González-Jiménez

Universidad Autónoma de Madrid

Let $\Phi_{\mathbb{Q}}(d)$ be the set of possible isomorphic torsion structures $E(K)_{\text{tors}}$, where K runs through all number fields K of degree d and E runs through all elliptic curves over $\mathbb{Q}$. The case $\Phi_{\mathbb{Q}}(d)$ where $d = 2, 3, 4, 5, 7$ or d is not divisible by $2, 3, 5, 7$ have been completely settled (in a serie of papers by A. Lozano-Robledo, F. Najman, J.M. Tornero, and the author).

The aim of our project is to shed light on what $\Phi_{\mathbb{Q}}(d)$ could be for other degrees d. For this purpose we have developed a fast algorithm that takes as input an elliptic curve defined over $\mathbb{Q}$ and an integer d and returns all the number fields K of degree dividing d such that $E(K)_{tors}$ contains $E(F)_{tors}$ as a proper subgroup, for all $F \subseteq K$. We have run this algorithm for all elliptic curves in LMFDB (or Cremona's database) and all $d \leq 23$ (in progress), collected various interesting data and found along the way new examples of sporadic points on modular curves $X_1(m, n)$, for $m \geq 2$. In particular, we found a degree 6 sporadic point on $X_1(4, 12)$, which is so far the lowest known degree a sporadic point on $X_1(m, n)$, for $m \geq 2$.

This is an ongoing project with F. Najman.

Automorphism groups of modular curves and torsion subgroups of elliptic curves

Daeyeol Jeon

Kongju National University

In this talk, we consider the problem to compute the automorphism groups of certain modular curves and its application to construct elliptic curves with given torsion subgroup structures over Galois extensions of the rational number field.

Some cases of Serre's uniformity problem

Pedro Lemos

Max Planck Institute for Mathematics, Bonn

Given a number field K, Serre's uniformity question asks whether there exists a constant C_K (depending only on K) such that if E/K is an elliptic curve without complex multiplication, then $\bar{\rho}_{E,p}$ is surjective for every prime $p > C_K$. In this talk, using ideas of Darmon and Merel, I will show that if $E/\mathbb{Q}$ is an elliptic curve without complex multiplication and for which there exists a prime ℓ such that $\bar{\rho}_{E,\ell}$ is contained in a Borel or in the normaliser of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, then $\bar{\rho}_{E,p}$ surjects onto $\mathrm{GL}_2(\mathbb{F}_p)$ for every prime $p > 37$. We will also discuss how to adapt arguments of Ellenberg in order to show a similar result in the case of $\mathbb{Q}$-curves completely defined over quadratic fields and satisfying analogous conditions.

A classification of p-adic Galois representations attached to elliptic curves with CM

Álvaro Lozano-Robledo

University of Connecticut

The goal of this talk is to give an explicit classification of the possible p-adic Galois representations that are attached to elliptic curves E with CM defined over $\mathbb{Q}(j(E))$. More precisely, let K be an imaginary quadratic field, and let $\mathcal{O}_f$ be an order in K of conductor $f \geq 1$. Let E be an elliptic curve with CM by $\mathcal{O}_f$, such that E is defined by a model over $\mathbb{Q}(j(E))$. Let $p \geq 2$ be a prime, let $G_{\mathbb{Q}(j(E))}$ be the absolute Galois group of $\mathbb{Q}(j(E))$, and let $\rho_{E,p}\colon G_{\mathbb{Q}(j(E))} \to \mathrm{GL}(2,\mathbb{Z}_p)$ be the Galois representation associated to the Galois action on the Tate module $T_p(E)$. Our goal is to describe, explicitly, the groups of $\mathrm{GL}(2,\mathbb{Z}_p)$

that can occur as images of $\rho_{E,p}$ for an arbitrary order $\mathcal{O}_f$. We will also discuss applications of the classification to the study of fields of definition of torsion structures of elliptic curves with CM.

Current methods versus expectations in the asymptotic of uniform boundedness

Loïc Merel

Institut de Mathématiques de Jussieu Paris Rive Gauche, Université Paris Diderot

The torsion primes for elliptic curves over algebraic number fields of degree d are bounded, according to the best current knowledge, exponentially in d. A disappointing result as polynomial bounds are expected.

Still the proof of the uniform boundedness can teach us something about a polynomial improvement. Recall that it is organized as follows. Consider E an elliptic curve over a number field K (of degree d over $\mathbf{Q}$) with a torsion point P or prime order p. Choose an arbitrary prime number l (not 2). A paradoxical dichotomy presents itself.

- In the easy cases, e.g. when E has potentially good reduction at some prime above l, one finds $p < (1 + l^{d/2})^2$ (the obviously exponential Hasse-Weil bound).
- The remaining situations constitute the hard cases. They happen when, at all primes of K above l, E does not have potentially good reduction and P extends to a point of order p in the component group of the special fiber of the Néron model of E (this is easier to grasp geometrically: it means that, if we designate by $< P >$ the cyclic subgroup of E defined by P, the conjugates of $(E, < P >)$ define a point Q of the d-th symmetric power $X_0(p)^{(d)}$ of the modular curve such that Q specializes to the d-th power of the cups 0. We say that Q is 0 totally cuspidal at l.). Then p is bounded polynomially in d. The best known bound seems due to Parent and Oesterlé who proved that there exists $C > 0$ independent of l such that $p < Cd^6$. The method relies on certain analytic number theoretic results.

In the lecture, we will revisit the proof by introducing certain auxiliary level structures, that will enable us to bypass completely analytic number theory. Thus we will see how to best improve the polynomial bound of Parent and Oesterlé in the hard cases. Our main aim is to highlight what are the limits of the current method, and, unfortunately, how those limits fall short of expectations.

Stable models for modular curves in prime level

Pïerre Parent
University of Bordeaux

We describe stable models for modular curves associated with all maximal subgroups in prime level, including the new case of non-split Cartan curves. (Joint work with Bas Edixhoven.)

Reductions of points on elliptic curves

Antonella Perucca
University of Luxembourg

Consider an elliptic curve over a number field K, and a K-rational point α of infinite order. We reduce α modulo the primes $\mathfrak{p}$ of K of good reduction, and consider the order of α modulo $\mathfrak{p}$. How likely is it that this (finite) order is odd, or more generally that it is coprime to some fixed integer m? The aim is understanding and computing the corresponding Dirichlet density of primes of K. The origin of this problem goes back to Hasse in the sixties and substantial progress has been made by Jones and Rouse in 2010. In this talk we present recent work with Davide Lombardo (2017) and with Peter Bruin (2018). We provide formulas that do not require additional assumptions and prove that the density is a theoretically computable rational number whose minimal denominator can be bounded in a uniform way.

A moduli interpretation for the non split Cartan modular curves : necklaces

Marusia Rebolledo
Université Blaise Pascal Clermont–Ferrand

Here, we are interested in the modular curves associated to non split Cartan subgroups or their normalizer in $\mathrm{GL}_2(\mathbb{F}_p)$. These modular curves appear for instance in Serre's problem of classifying all possible Galois structures of p-torsion points on elliptic curves over number fields. With Christian Wuthrich, we proposed a description of those curves as moduli spaces, namely classifying elliptic curves endowed with a level structure that we call a necklace. I will show how this description allows to recover some classical results (on elliptic points, degenerate maps, Hecke operators etc) as well as it gives a more explicit and geometric vision of a theorem of Chen.

Progress on Mazur's program B, part II: equations of modular curves

Jeremy Rouse
Wake Forest University

In this talk, we discuss an efficient method for computing equations of modular curves attached to arbitrary congruence subgroups. Given a subgroup H of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ containing $-I$, we compute a basis for the space of weight 2 Eisenstein series on H built from specializations of the Weierstrass $\wp$-function. These have the feature that it is easy to explicitly compute the action of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ on the basis functions, which facilitates computing the function field of the modular curve X_H as an extension of the function field of $X_{\tilde{H}}$ for some subgroup $\tilde{H} \supseteq H$. We use this to give equations for the arithmetically maximal 2-power level modular curves, and the level 17 modular curve corresponding to the normalizer of a non-split Cartan subgroup.

Torsion points of an elliptic curve over $\mathbb{Q}(\sqrt{37})$

René Schoof
University of Rome Tor Vergata

Up to isogeny, there is a unique elliptic curve over $\mathbb{Q}(\sqrt{37})$ with good reduction everywhere. We discuss the conjecture that this is actually the only abelian variety over $\mathbb{Q}(\sqrt{37})$ with good reduction everywhere.

Primitivity of points on elliptic curves

Peter Stevenhagen
University of Leiden

For an element in the multiplicative group of a number field K that is globally primitive, i.e., not an n-th power in K^* for any integer $n > 1$, one can show that, under GRH, the set of primes of K for which the reduction generates the multiplicative group of the residue class field has positive density.

For a globally primitive point on an elliptic curve E/K, it can however happen that the set of primes for which the reduced point generates the point group over the residue class field is finite, even in cases where $E(K)$ is torsionfree. We discuss the Galois representations that give rise to this unusual behavior.

This is joint work with Francesco Pappalardi (Rome) and Nathan Jones (Chicago).

Simultaneous torsion in the Legendre family of elliptic curves

Michael Stoll
University of Bayreuth

Let $\alpha, \beta \in \mathbb{C} \setminus \{0, 1\}$ be distinct, and define $T(\alpha, \beta)$ to be the set of parameters $\lambda \in \mathbb{C} \setminus \{0, 1\}$ such that the points with x-coordinate α and β are torsion on the Legendre elliptic curve $y^2 = x(x-1)(x-\lambda)$.

Masser and Zannier have shown that $T(\alpha, \beta)$ is always finite. We will present some results regarding effectivity of $T(\alpha, \beta)$; for example, we show that the set can be effectively determined when α and β are both algebraic and not too close 2-adically. We also show that $T(\alpha, \beta)$ has at most one element when $\mathbb{Q}(\alpha, \beta)$ has transcendence degree 1. Based on this result, we obtained a large amount of experimental data, and we will present some conjectures that are suggested by this.

Counting points on modular curves

Andrew Sutherland
Massachusetts Institute of Technology

I will present a new algorithm for counting points on modular curves over finite fields that is faster (and more general) than previous methods, building on ideas of Zywina that were exploited in our prior joint work. A key feature of this algorithm is that it does not require a model of the curve. I will then describe how this can be used to compute the L-function of the curve, thereby obtaining an upper bound on the analytic rank of the Jacobian that is provably tight when it is less than 2.

Torsion groups of elliptic curves over quadratic fields $\mathbb{Q}(\sqrt{d}),\ 0 < d < 100$

Antonela Trbović
University of Zagreb

We describe methods for proving results towards classifying the possible torsion subgroups of elliptic curves over quadratic fields $\mathbb{Q}(\sqrt{d})$, where $0 < d < 100$ is a square-free integer, and obtain a complete classification for 49 out of 60 such fields. Over the remaining 11 quadratic fields, we cannot rule out the possibility of the group $\mathbb{Z}/16\mathbb{Z}$ appearing as a torsion group of an elliptic curve.

On Fermat's equation over some quadratic imaginary number fields

George Turcas

Warwick University

Assuming a deep but standard conjecture in the Langlands programme, we prove Fermat's Last Theorem over $\mathbb{Q}(i)$. Under the same assumption, we also prove that, for all prime exponents $p \geq 5$, the Fermat's equation $a^p + b^p + c^p = 0$ does not have non-trivial solutions over $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-7})$. In the proof of these theorems we use results concerning upper-bounds for possible prime torsion that can be achieved by elliptic curves over number fields of small degree to prove irreducibility of some residual Galois representations. Time permitting, we will discuss work in progress towards proving similar theorems over other quadratic imaginary number fields of class number 1.

Prime-to-p actions of inertia associated to semistable hyperelliptic curves

Jeff Yelton

Universtiy of Milan

To any hyperelliptic curve C over a field K (defined here to include the case of elliptic curves), we consider the ℓ-adic representation coming from the natural Galois action on the ℓ-adic Tate module of its Jacobian. When K is a local field with residue characteristic p, I will discuss an approach to determining the restriction of this ℓ-adic action to the inertia subgroup I for each prime ℓ different from p, using a joint result with H. Hasson that describes the action of I on the prime-to-p etale fundamental groups of punctured projective lines. In the case of semistable elliptic curves, this gives a slightly more explicit form of the description we know from Tate's theory of p-adic uniformization. If time permits, I will present some results on global ℓ-adic Galois images which arise as direct applications of this description of the inertia action.

Progress on Mazur's program B, part III: rational points

David Zureick-Brown
Emory University

I'll discuss recent progress on Mazur's ”Program B” – the problem of classifying all possibilities for the "image of Galois" for an elliptic curve over $\mathbb{Q}$ (equivalently, classification of all rational points on certain modular curves X_H), with a focus on the aspects related to provably compute the rational points on the modular curves X_H.

This will including my own recent work with Jeremy Rouse which completely classifies the possibilities for the 2-adic image of Galois associated to an elliptic curve over the rationals. I will also discuss a large number of other very recent results by many authors.

Index

Anni, S., 12

Barbulescu, R., 12
Bourdon, A., 13
Bruin, P., 13

Chou, M., 14
Clark, P., 14

Daniels, H., 15
Derickx, M., 15
Dokchitser, V., 16

Fisher, T., 16
Frey, L., 16

Garnek, J., 17
Gonzalez-Jimenez, E., 17

Jeon, D., 18

Lemos, P., 18
Lozano-Robledo, Á., 18

Merel, L., 19

Parent, P., 20
Perucca, A., 20

Rebolledo, M., 20
Rouse, J., 21

Schoof, R., 21
Shinde, S., 12
Stevenhagen, P., 21
Stoll, M., 22
Sutherland, A., 22

Trbović, A., 22
Turcas, G., 23

Yelton, J., 23

Zureick-Brown, D., 24