MODERN TOOLS FOR RATIONAL POINTS ON CURVES OVER FINITE FIELDS

STEFANO MARSEGLIA, CHRISTOPHE RITZENTHALER, AND ANNA SOMOZA

Abstract. This is a tryptic of courses whose goal is to provide modern tools to address research challenges on rational points over finite fields. Although the courses are related, each of them can be appreciated on its own and considered as a nice introduction to a classical topic in arithmetic or algebraic/analytic geometry.

1. How to apply?

The videos and notes of the courses will be available to everyone. However in order to be able to have interactions with each student as in a real class, we will also set up a chat platform and organize video sessions. We therefore want to limit the number of participants to 50. The courses are primely directed to Turkish students under the supervision of Alp Bassa from Boğaziçi University but we open them to some young (Master, PhD or post-docs) participants from other developing countries.

Please note that online teaching and learning require a great commitment: do not apply if you are not ready and available to devote time to study and participate actively to the classes.

If needed, selected candidates can benefit from CIMPA support to acquire a good connection or buy small equipment to participate to the courses in good conditions.

2. How will the course take place?

Starting beginning of March, we will release a series of videos which will contain the material of the courses in addition to notes. You will have time to study these videos and courses till May. In order to assist you during that time, a chat platform will be set up so that you can ask your questions to the lecturers and also work in groups. At the same time, exercises will be suggested so that you can learn by doing (best way!) and video tutorial sessions will be organized so that you can present your solutions in turn.

Finally, depending on the evolution of the pandemic, we hope to end the courses with a 2 weeks face-to-face research workshop in Turkey where the most successful students will be invited to participate.

3. Description of the courses

3.1. **Geometry and arithmetic of low genus curves and relations with their Jacobian (Ritzenthaler).** The course will largely follow these notes to which we refer for a more detailed description of the content.

Date: February 1, 2021.

The first purpose is to introduce/recall basic properties of algebraic curves in order to be able to describe precisely these curves up to genus 5. Having this geometric description will be a first step to control their arithmetic.

We will then study Weil's conjectures for curves over finite fields and various corollary: these results encode deep control on the number of rational points. In particular, we will see that they give non-trivial bounds for the number of points.

In order to construct low genus $g > 0$ curves with many rational points, the most powerful strategy is to work with their Jacobian. This is a a g-dimensional variety which understanding or description requires more advanced knowledge in algebraic geometry. Somoza's course will consider these objects over the complex and will give the necessary intuition to follow this part of the course. In turn, this part of the course will serve as foundation for the second part of Marseglia's lecture.

References: please have a look at the notes. In brief, having studied basic algebraic geometry may ease your way into the course.

Specificity of the lectures: As the notes already exist, the videos won't be a rewriting of the notes on the blackboard. The lecturer will motivate the study of each chapter, clarify some difficulties (for instance by giving details on a long example), and give further connections and illustrations.

3.2. **Ideal Class Monoid and computing abelian varieties over finite fields (Marseglia).** The aim of this course is to describe an algorithm that given an isogeny class of abelian varieties over $\mathbb{F}_q$ returns the isomorphism classes within it. The main tool is that, under certain hypotheses on the isogeny class, we can functorially describe the abelian varieties in terms of fractional ideals of orders in étale algebras over $\mathbb{Q}$ (product of number fields).

The course is divided into two parts:

(1) Fractional ideals of maximal orders of number fields and the group of their isomorphism classes (class group) are at the core of algebraic number theory. They are heavily studied and there are efficient algorithms to compute them. The situation gets a lot more complicated when the order in consideration is non-maximal: there will be fractional ideals that are not invertible and so their classes will not form a group but just a monoid. In this part of the course we will start by stating the basic definition of étale algebras over $\mathbb{Q}$, orders and fractional ideals. We will continue by proving their main properties and conclude by giving an algorithm to compute the ideal classes of a given order.

    This part of the course is rather self-contained and requires only mild prerequisites from commutative algebra.

(2) The second part of the course, which builds on Ritzenthaler and Somoza's lectures, will be about the abelian varieties over finite fields. In general, such varieties are 'wilder' than their complex counterpart, and there are several invariants attached to them that are not well understood. Our goal is to give an overview of the most useful tools to study them: Tate modules, isogeny classification, functorial descriptions in terms of modules with a "Frobenius"-like endomorphism. Under certain assumptions, such modules will be fractional ideals: this is a great news because from the first part we know how to compute them (up to isomorphism)!

    Contrary to the first, in this second part of the course we will only reference or sketch the proofs of some of the deeper results we will encounter.

Main References:

First part: S. Marseglia, *Computing the ideal class monoid of an order*, J. Lond. Math. Soc. 101 (2020), no. 3, 984-1007, available at https://arxiv.org/abs/1805.09671

Second part: S. Marseglia, *Computing square-free polarized abelian varieties over finite fields*, Mathematics of Computation 90 (2021), no. 328, 953–971, available at https://arxiv.org/abs/1805.10223

3.3. **Complex abelian varieties (Somoza).** The aim of this course is to give an introduction to abelian varieties over the complex numbers, starting from dimension 1, that is, complex elliptic curves, which we will present as motivation for the course.

The main object we will work with is the complex torus, that is, the quotient of a complex vector space by a full-rank lattice. We will see that complex abelian varieties are complex tori, and characterize when a complex torus is an abelian variety. As an example, we will introduce the Jacobian of a curve, see how to construct it as a complex abelian variety, and define Riemann theta functions and their role in relating a curve with its complex Jacobian.

As an application, we will venture into the theory of complex multiplication: we will see how one can construct abelian varieties with this property, and how to use this construction together with Riemann theta functions in order to obtain equations of curves with interesting properties.

References:

As motivation for the course:

Chapter 6 in J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edition, Graduate Texts in Mathematics, Springer New York, 2009.

Other references:

M. Rosen, *Abelian Varieties over* $\mathbb{C}$. In: Cornell G., Silverman J.H. (eds) Arithmetic Geometry. Springer, New York, NY.

C. Birkenhake and H. Lange, *Complex Abelian Varieties*. volume 302 of Grundlehren der Mathematischen Wissenschaften. Springer-Verlag, Berlin, second edition, 2004.

Stefano Marseglia, Utrecht University, P.O. Box 80010, 3508 TA, Utrecht, The Netherlands.
Email address: s.marseglia@uu.nl

Christophe Ritzenthaler, Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France.
Email address: christophe.ritzenthaler@univ-rennes1.fr

Anna Somoza, Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France.
Email address: anna.somoza.henares@gmail.com