FOCM 2014 - Workshop A3
Computational Number Theory

A3 - December 11, 14:30 – 15:10

Class invariants for abelian surfaces

Andreas Enge
INRIA Bordeaux-Sud-Ouest, France
andreas.enge@inria.fr

Abelian surfaces, or equivalently Jacobians of genus 2 hyperelliptic curves, are the "next complex" case of abelian varieties after elliptic curves, and a serious contender for fast implementations of cryptosystems based on the discrete logarithm problem. Complex multiplication provides an interesting way of obtaining such surfaces with a known number of points over a finite field; it requires the costly computation of a large polynomial defining a certain class field.

I will report on joint work with Emmanuel Thomé on an asymptotically quasi-linear algorithm to compute such class polynomials with floating point approximations, as well as on its freely available implementation. Then I will present joint work with Marco Streng on a systematic approach for obtaining class invariants, that is, elements of the same class field with smaller minimal polynomials, and show how to solve the problem of obtaining all their algebraic conjugates in an easy way.

Joint work with Emmanuel Thomé (INRIA Nancy-Grand Est, France) and Marco Streng (Universiteit Leiden, Netherlands).

A3 - December 11, 15:10 – 15:50

Aspects of Belyi maps

Jeroen Sijsling
Dartmouth College, United States of America
sijsling@gmail.com

A Belyi map is a finite morphism to the complex projective line that is branched above at most three points. Surprisingly, the algebraic curves that admit a Belyi map are exactly those that are defined over the algebraic closure of the rationals. Due to the simple combinatorial description of covers as finite sets with an action of the fundamental group, the theory of Belyi maps therefore gives a way to study the absolute Galois group of the rationals, one of Grothendieck's dreams.

This talk will explain the links between Belyi maps and other areas of study, such as Shimura curves, inverse Galois theory, and number fields with small ramification. Hopefully this will make show how Belyi maps, like (and linked with) modular forms, can be a useful tool for any computationally inclined number theorist. Finally, the currently available techniques to compute Belyi maps are described, including a recent one due to Klug, Musty, Schiavone and Voight.

Joint work with John Voight.

A3 - December 11, 15:50 – 16:30

Distribution of traces of genus 3 curves

Christophe Ritzenthaler
University Rennes 1, France
ritzenthalerchristophe@gmail.com

We present numerical experiments to visualize the asymmetry in the distribution of traces of Frobenius of genus 3 curves over finite fields. These observations are linked to the so-called Serre obstruction for non hyperelliptic curves. We also give a heuristic explaination for the phenomena we observe.

Joint work with Reynald Lercier (university Rennes 1), Florent Rovetta (university Aix-Marseille), Jeroen Sijsling (Dartmouth college) and Ben Smith (Polytechnique Paris).

A3 - December 11, 17:05 – 17:55

Polynomial time computation of Galois representations attached to modular forms.

Bas Edixhoven
Universiteit Leiden, Netherlands
edix@math.leidenuniv.nl

Modular forms give rise to number fields with non-solvable Galois groups, acting faithfully on finite subgroups of jacobian varieties of curves. In joint work with Couveignes, de Jong and Merkl, generalised by Bruin, it was shown that these number fields can be computed in polynomial time. The major difficulty is that such computations must be done in time polynomial in the dimension of the jacobian varieties that arise. This difficulty was solved by approximate computations and bounds that allow us to get exact solutions from approximate ones. The bounds will be discussed briefly. We will focus on Couveignes's algorithms for the approximate computations. Finally, real computations by Bosman, Mascot, Zeng, Derickx, van Hoeij and Peng will be presented.

Joint work with Jean-Marc Couveignes (Université Bordeaux 1), Robin de Jong (Universiteit Leiden), Franz Merkl (Universität München) and Peter Bruin (Universiteit Leiden).

A3 - December 11, 18:00 – 18:40

Computations on a conjecture of BSD type postulated by B. Mazur and J. Tate

Francisco Portillo
UACM, Mexico
francisco.portillo@uacm.edu.mx

In a series of articles, Mazur and Tate postulated a p-adic analogue of the Birch and Swinnerton-Dyer conjecture for finite layers. This conjecture have similar invariants as the classical BSD conjecture, but it has a multiplicative form. Invariants like the Tamawaga numbers, the order of the torsion, the order of the Tate-Shafarevich group, appear as exponents of the arithmetic side of the conjectured equation. In the analytic side, we have Modular Symbols that play the role of the $\mathcal{L}$ function, and the equation holds over a finite abelian multiplicative group. We will present computational evidence in favor of the mentioned conjecture, and we will explain how it was computed.

A3 - December 12, 14:30 – 15:10

All del Pezzo surfaces of degree two over finite fields are unirational

Cecilia Salgado
UFRJ, Brazil
salgado@im.ufrj.br

A consequence of the Segre-Manin theorem is that a del Pezzo surface of degree two is unirational over its base field as long as it possesses a general rational point defined over the field in question. In this work, joint with D. Testa and A. Várilly-Alvarado, we show that all del Pezzo surfaces of degree two over a finite fields are unirational with at most three possible exceptions. Recently, Festi and van Luijk showed that these three last surfaces are also unirational. I will discuss the arguments involved in our proof.

Joint work with Damiano Testa (Warwick, UK) and Anthony Várilly-Alvarado (Rice, USA).

A3 - December 12, 15:10 – 15:50

Concurrent lines on del Pezzo surfaces of degree one

Ronald van Luijk
Universiteit Leiden, Netherlands
rmluijk@gmail.com

Let k be a field and $\overline{k}$ an algebraic closure. A del Pezzo surface over k is a surface over k that is isomorphic over $\overline{k}$ to either $\mathbb{P}^1 \times \mathbb{P}^1$ (degree 8), or $\mathbb{P}^2$ blown up at $r \leq 8$ points in general position (degree $9 - r$). Famous examples (with $r = 6$ and degree 3) are smooth cubic surfaces in $\mathbb{P}^3$, which over $\overline{k}$ contain 27 lines; at most three of these can be concurrent, that is, go through the same point. Analogously, we get 240 lines for $r = 8$ and degree 1. Based on the graph on these lines, with edges between those that intersect, we get an upper bound of 16 for the number of concurrent lines. We show that this upper bound is only attained in characteristic 2, which makes the case $r = 8$ different from all other cases. In most characteristics, including characteristic 0, the upper bound is 10.

Joint work with Rosa Winter (Universiteit Leiden, Netherlands).

A3 - December 12, 15:50 – 16:30

Computing twists of Shioda modular surfaces of level 4 related to visibility of Sha

Nils Bruin
Simon Fraser University, Canada
nbruin@sfu.ca

One of the most mysterious objects associated to an elliptic curve E is its Tate-Shafarevich group $Sha(E)$. Its elements can be represented by classes in the Galois-cohomology group $H^1(Q, E[n])$, for various n.

If two distinct elliptic curves E and E' have isomorphic n-torsion, then a single class ξ in $H^1(Q, E[n])$ can represent a trivial element in $Sha(E)$ and a non-trivial one in $Sha(E')$. In the terminology of Mazur, the element of $Sha(E')$ is made *visible* by E. Mazur showed that for $n = 3$, all elements of Sha can be made visible. In general, the question translates into whether a rational point lies on a certain twist of the Shioda modular surface, obtained by taking the universal elliptic curve over the modular curve $X(n)$ of full level n.

The case $n = 4$ is particularly interesting. The curve $X(4)$ is rational, but the relevant surface over it is not. It is a K3 surface. Further complications in determining the correct surface arise from the fact that 4 is even. We will discuss how to compute a model of the relevant surface given ξ and give some examples of the various obstructions to rational points that can arise on these surfaces.

Joint work with Tom Fisher (Cambridge, United Kingdom).

A3 - December 12, 17:00 – 17:40

Prime densities for GL_1 and GL_2

Peter Stevenhagen
Universiteit Leiden, Netherlands
psh@math.leidenuniv.nl

If we fix a rational number x, Artin's basic question "for how many primes p does x mod p generate the multiplicative group of non-zero integers modulo p?" leads to Artin's conjecture on primitive roots, and the associated prime density depends in a somewhat non-trivial way on x. A conceptual way to compute such densities is given by the character sum method that I developed with Moree and Lenstra, and that exploits Galois representations coming from the multiplicative group.

Artin-type questions also exist in an elliptic setting, as do the associated Galois representations. I will explain how our character sum method extends to this case.

Joint work with Pieter Moree (Max Planck Institut Bonn) and Hendrik Lenstra (Universiteit Leiden).

A3 - December 12, 17:40 – 18:20

Computing tables of elliptic curves

Ariel Pacetti
UBA, Argentina
apacetti@dm.uba.ar

In modern computational number theory, the existence of tables of elliptic curves plays a central role. They allow to test many open conjectures and give some hint on the behavior of rank and many other quantities of elliptic curves as the conductor grows.

The main contribution on elliptic curves' tables are Cremona's tables, which are based con computing modular symbols and the action of the Hecke operators on them. The problem is that elliptic curves correspond to rational eigenvalues, while most eigenvalues are not rational, so the cost of computing the whole Hecke operators is too big for the few curves obtained. There is a variant due to Cremona-Lingham, which consists on computing j-invariants over number fields, and have some computational cost. In this talk we will present a different approach which consists on using information of the residual 2-adic representation. This allows to speed up computations assuming some conjectures on minimal models up to isogenies. This is a work in progress, and the ideas presented should be generalizable to arbitrary number fields.

A3 - December 13, 14:30 – 15:10

On the number of points of Jacobians over finite fields: from asymptotic theory to applications

Alexey Zykin
Université de la Polynésie française, France
alzykin@gmail.com

Asymptotic theory of global fields was developed by Tsfasman and Vladuts in 1990's in connection with the problem of bounding the number of points on varieties over finite fields and its applications to the coding theory. In my talk I will explain how explicit versions of Tsfasman and Vladuts results (namely, that of the generalized Brauer-Siegel theorem) can be used for getting very tight bounds for the number of points on jacobians of curves over finite fields. If time permits, I will discuss some progress in finer asymptotic questions related to the asymptotically bad situation in the case of cyclotomic fields and modular curves. This is a joint work with Philippe Lebacque.

Joint work with Philippe Lebacque (Université de Franche-Comté, France).

A3 - December 13, 15:10 – 15:50

Arithmetic geometry and key exchange : compact Diffie–Hellman with efficient endomorphisms

Benjamin Smith
INRIA and École polytechnique, France
smith@lix.polytechnique.fr

Diffie–Hellman key exchange is one of the fundamental primitives in public-key cryptography. If G is an abelian group (written additively), then the Diffie–Hellman protocol in G is composed of four computations in the form $P \longmapsto [m]P = P + \cdots + P$ (m times) for various points P and integers m; optimising this scalar multiplication operation is crucial.

In practice, the most efficient contemporary Diffie–Hellman implementations are based on elliptic curves, or Jacobians of genus 2 curves. But in these groups, computing $-P$ is extremely efficient, so we can use the fact that $[m](\pm P) = \pm([m]P)$ to simplify and speed up the protocol, identifying P with $-P$ (formally, working in the quotient set $G/\langle\pm 1\rangle$). These "compact" systems offer significant savings in both space, which translates into slightly shorter keys, and in computing time, through simpler pseudo-group law formulae. In the elliptic curve context, this amounts to using only x-coordinates of points and Montgomery's pseudo-group law. Bernstein's Curve25519 software, which has become a de facto reference implementation of Diffie–Hellman at the 128-bit security level, is a practical example of these techniques in practice. The genus 2 analogue is Kummer surface arithmetic, where we can use particularly efficient formulae developed by the Chudnovskys, and popularized in cryptography by Gaudry.

Recent years have seen renewed interest in the Gallant–Lambert–Vanstone (GLV) technique for computing $[m]P$ in G. Here, we suppose our elliptic curve (or our genus 2 Jacobian) has an efficiently computable non-integer endomorphism ϕ, which when applied to elements of G acts like $[\lambda]$ (for some large eigenvalue λ). Suppose we want to compute $[m]P$: first we use the Euclidean algorithm to compute much smaller integers a and b such that $a + b\lambda \equiv m \pmod{\#G}$, and then we compute $[m]P = [a]P + [b]\phi(P)$. The running time of the multiexponentiation depends on the size of a and b, while traditional scalar multiplication depends on the size of m. In practice, a and b have half the bitlength of m, which means that GLV and its variants can offer us a significant speedup.

In this talk, we will discuss the adaptation of GLV techniques to x-coordinate-only and Kummer surface systems. On the practical side, we will present recent experimental results for a new elliptic-curve based implementation. On the more theoretical side, we will present some new formulae for Kummer surface systems.

A3 - December 13, 15:50 – 16:30

Paramodular forms: central values of twisted spin L-functions

Gonzalo Tornaria
Universidad de la República, Uruguay
tornaria@cmat.edu.uy

In the 1980s Böcherer formulated a conjecture relating the central values of the imaginary quadratic twists of the spin L-function attached to a Siegel modular form F to the Fourier coeficients of F.

In this talk I will present some recent generalizations of this conjecture to the case of paramodular forms, and the computations providing numerical evidence for the new conjectures.

Joint work with Nathan Ryan (Universidad de la República / Bucknell University).

A3 - December 13, 17:00 – 17:40

Hypergeometric Motives

Fernando Rodriguez Villegas
Abdus Salam International Center for Theoretical Physics, Italy
villegas@ictp.it

The families of motives of the title arise from classical one-variable hypergeometric functions. This talk will focus on the calculation of their corresponding L-functions. These represent a fairly wide class of L-functions that are numerically accessible going well beyond standard cases.

Joint work with Frits Beukers (University of Utrecht), Henri Cohen (Universite de Bordeaux), Anton Mellit (ICTP), David Roberts (University of Minnesota, Morris), Masha Vlasenko (University College Dublin) and Mark Watkins (MAGMA group, University of Sydney).

A3 - December 13, 17:40 – 18:20

Torsion structures of elliptic curves over number fields

Filip Najman
University of Zagreb, Croatia
fnajman@math.hr

We say that a torsion structure on an elliptic curve over a number field K is either a K-rational torsion subgroup or a $\mathrm{Gal}(\overline{K}/K)$-invariant cyclic subgroup (which is also the kernel of a cyclic isogeny defined over K) of E. Recent years have seen a great deal of progress in many directions, by work of many people, in understanding torsion structures of elliptic curves over number fields.

I will talk about some of these recent results: which torsion structures are possible over number fields of fixed degree or over certain fixed number fields, about elliptic curves with special“ torsion structures and how they were constructed, which properties can prescribing the torsion structure imbue on an elliptic curve with that torsion structure, and about the number of twists with large torsion that an elliptic curve can have.

Joint work with Peter Bruin (Universiteit Leiden, Netherlands).

A3 - Poster

Congruences between modular forms modulo prime powers

Maximiliano Javier Camporino
Universidad de Buenos Aires, Argentina
mcamporino@dm.uba.ar

Consider the following problem: given a modular form f and a prime power p^n, is there a modular form g, different from f, such that f and g are congruent modulo p^n?. A way to solve this problem is to consider the Galois representation attached to f, take its modulo p^n reduction and study the obstructions appearing when trying to lift it back to a ring of characteristic zero. In this way, we obtain a local-to-global lifting result for abstract representations, which, when combined with the appropiate modularity lifting theorem, translates into an affirmative response for the proposed problem. Moreover, the method provides a way to control the local behavior of the representations (and hence the modular forms) constructed, giving applications to level lowering and level raising problems.

We can show in a concrete example how the method works, getting a case of modulo p^n level raising. We find a congruence modulo 25 between an elliptic curve of conductor 17 and a modular form of level $17 \cdot 113$. The obtainment of this example involves computing groups of Galois cohomology of the representation attached to the elliptic curve and understanding the local behavior of the elements lying inside them. For this, we compute abelian extensions of a high degree Galois extension of $\mathbb{Q}$, which turns out to be a computationally challenging problem.

Joint work with Ariel Pacetti (Universidad de Buenos Aires, Argentina).

A3 - Poster

Heegner Points on Cartan non-split Curves

Daniel Kohen
IMAS-CONICET , Argentina
kohendaniel@gmail.com

The goal is to construct Heegner Points on elliptic curves over $\mathbb{Q}$ in cases where the classical Heegner hypothesis does not hold. Concretely, let $E/\mathbb{Q}$ be an elliptic curve of conductor N , p an odd prime such that p^2 divides N exactly, and K an imaginary quadratic field in which p is inert and the other primes dividing the conductor are split. In this case there aren't any Heegner points in the modular curve $X_0(N)$, but since $sign(E/K) = -1$ we still expect to somehow construct "Heegner points". The idea is to consider other modular curves, the so called Cartan non-split curves, whose Jacobian is isogenous to the new part of $J_0(p^2)$. In order to compute the Abel-Jacobi map we need to compute the Fourier expansions of newforms associated to Cartan non-split groups. These Fourier expansions have coefficients in $\mathbb{Q}(\xi_p)$ and, under a situable normalization, the coefficients satisify nice properties when congujated by elements of $Gal(\mathbb{Q}(\xi_p)/\mathbb{Q})$. This allows us to construct Heegner points for these Cartan groups. We also show many examples of our construction in cases where they generate the Mordell-Weil group, and relate them to the BSD conjecture. This is based on the work done in http://arxiv.org/abs/1403.7801 .

Joint work with Ariel Pacetti (Universidad de Buenos Aires, Argentina).
