# AGCT-13 Conference

## Arithmetic, Geometry, Cryptography and Coding Theory

**March 14th-18th 2011**

C.I.R.M. - France

**Yves Aubry, Christophe Ritzenthaler and Alexey Zykin**

## Program and abstracts

| | Monday | Tuesday | Wednesday | Thursday | Friday |
|---|---|---|---|---|---|
| 9.00 - 10.00 | Howe | Hindry | Stichtenoth | Serre | Shioda |
| 10.00 - 10.30 | Rökaeus | Salgado | Ballet | Wiese | Singh |
| 10.30- 11.00 | | | | | |
| 11.00 - 11h30 | Homma | Boyer | Mak | Baran | Rodier |
| 11.30 - 12h00 | Haloui | Bruin | Ozbudak | Khuri-Makdisi | Langevin |
| 12.30- 14.00 | Lunch | Lunch | Lunch | Lunch | Lunch |
| 14.00 - 14.30 | | | Junior | | Zarhin |
| 14.30 - 15.00 | | | | | Edoukou |
| 15.00 - 15.30 | | | | | Garcia |
| 16.00 - 17.00 | Blache | Viray | Mathematics | Couvreur | |
| 17.00- 17.30 | Anglès | Kohel | | Leducq | |
| 17.30- 18.00 | | | | | |
| 18.00- 18.30 | Ghorpade | Smith | Afternoon | Leander | |
| 18.30- 19.00 | Ostafe | Kontogeorgis | | Lisonek | |
| 19.30- | Diner | Diner | Diner | Conference diner | Diner |

The Junior Mathematics Afternoon will consist of two conferences for highschool students:
14.15 - 15.00 **Daniel Augot: Quand** $1+1=0$**.**
15.45 - 16.30 **Pascal Véron: Cryptographie: théorie et pratique.**

# Abstracts.

**Bruno Anglès: Zeta values for $\mathbb{F}_q[T]$.** We study the arithmetic properties of the values of the Goss zeta function at negative integers.

**Stéphane Ballet: Asymptotics for the class number of certain families of algebraic function fields defined over any finite field**. We give lower bounds for the number of effective divisors of degree $\leq g-1$ of an algebraic function field of genus $g$ defined over a finite field. We deduce lower bounds and asymptotics for the class number, depending mainly on the number of places of a certain degree. We give examples of towers of algebraic function fields having a large class number.

**Burcu Baran: Computing a level-13 modular curve over $\mathbb{Q}$ via representation theory.** For any $n > 0$, let $X_{\mathrm{ns}}(n)$ denote the modular curve over $\mathbb{Q}$ associated to the normalizer of a non-split Cartan subgroup of level $n$. The integral points and the rational points of $X_{\mathrm{ns}}(n)$ are crucial in two interesting problems: the class number one problem and the Serre's uniformity problem. In this talk we focus on the genus-3 curve $X_{\mathrm{ns}}(13)$. It has no $\mathbb{Q}$-rational cusp (as for any level $n > 2$), so to compute an equation for this curve as a quartic in $\mathbb{P}^2_{\mathbb{Q}}$ we use representation theory. Our explicit description of $X_{\mathrm{ns}}(13)$ yields a surprising exceptional $\mathbb{Q}$-isomorphism to another modular curve. We also compute the $j$-function on $X_{\mathrm{ns}}(13)$; evaluating it at the known $\mathbb{Q}$-rational points, we obtain the expected CM values.

**Régis Blache: Different aspects of Artin-Schreier curves and coverings**. We consider different aspects of Artin-Schreier curves and coverings:

- first $p$-adic aspects of Artin-Schreier curves: we present old and recent results about the $p$-rank, $p$-torsion and Newton polygons attached to the $p$-divisible group of their Jacobian. We recast them in the different stratifications of moduli spaces of principally polarized abelian varieties due to Oort and others. We pay particular attention to the case $p = 2$, when Artin-Schreier curves are hyperelliptic.
- Then we give bounds on the number of rational points of an Artin-Schreier covering. We follow and generalize the arguments of Rojas and Wan who treat coverings of the projective line having one branch point. We describe a family of $\ell$-adic sheaves whose traces are these numbers of points over the base field $\mathbb{F}_q$ and its extensions. From Laumon's results on the Fourier- Deligne transform, and Deligne's fundamental results, we improve the classical bounds (coming from Weil's proof of the Riemann hypothesis for finite fields) by a factor $\sqrt{q}$ in many cases.

**Ivan Boyer: Factorization of polynomials over finite fields in deterministic time.** Let $P$ be a polynomial in $\mathbb{Z}[X]$. The factorization of $P$ modulo a prime $p$ in probabilistic polynomial-time is well-known. However, the situation in deterministic time isn't known in general. This talk is devoted to the study of families of polynomials for which such deterministic algorithms exist.

**Nils Bruin: Explicit descent setups**. The first step in computing the group of rational points on a Jacobian of an algebraic curve over a global field is to compute the free rank of that group. The most common method does that by computing a Selmer group. While in principle effectively computable, one needs to specify extra data to do so in practice. We will present a description of such data, called an explicit descent setup, that covers all cases in the literature to date.
It is surprising how little information explicit descent setups yield about Selmer groups in general. There are various additional obstructions one needs to deal with as well. In cases considered previously, many of these turn out to be trivial, but when one adapts these methods for Jacobians of smooth plane quartics then it is easy to find examples where these obstructions play a role.

**Alain Couvreur: Codes from rational surfaces.** The topic of this talk is Algebraic Geometry codes from surfaces. It is motivated by two observations. First, in the literature, many explicit examples of good codes from surfaces arise from rational surfaces. However, this property of rationality is never used for

studying them. Second, the usual approach consists in constructing codes from "well–known" surfaces, i.e. surfaces whose geometry is well understood and then check whether these codes are good.

In this talk, the strategy is the converse. We first look for the properties which should be expected from a surface in order to produce good codes. Then, we construct rational surfaces satisfying these particular properties by blowing up the projective plane at some closed points. The property of rationality is deeply used in the study of the corresponding codes since the estimate of the minimum distance is reduced to a point counting problem on families of plane curves. By this manner, codes beating the best codes of Andries Brouwer tables have been discovered.

**Frédéric Edoukou: Codes on quadric and Hermitian varieties II**. In 2007, during the workshop AGCT, we proposed three conjectures.
The first, on the fourth and the fifth weight of the codes defined by evaluating quadrics on the non-singular Hermitian surface.
The second, on the distribution of the first five weights of the functional codes defined on the non-singular Hermitian variety.
The third, on the number of points in the intersection of two quadrics with no common hyperplane.
In this talk we will first of all show the progress done regarding these conjectures. Secondly we will give some new information on the structure of the functional codes defined on quadric and Hermitian varieties. Finally we will formulate some new conjectures.

**Arnaldo Garcia: On explicit towers over finite fields.** We are going to present some good towers over finite fields. We are interested in the ratios of rational points by the genus. We also give at the end a new tower over nonprime fields with an exciting very big limit.

**Sudhir Ghorpade: Primitive Recursive Vector Sequences**. Recursive vector sequences, also known as word oriented LFSRs, are a nice and natural generalization of homogeneous linear recurrence sequences over finite fields, also known as LFSRs. There is an analogous notion of primitivity. We will discuss a conjecture concerning the enumeration of primitive recursive vector sequences of a given order over a given extension of a finite field. There is also an equivalent formulation in terms of certain Singer cycles in general linear groups. Moreover, the conjecture is closely related with a problem of Niederreiter (1995) about the number of splitting subspaces of a given dimension. These problems seem to be open in general. We will outline some recent progress and related developments.
A part of this talk is a joint work with Samrith Ram.

**Safia Haloui: The characteristic polynomials of abelian varieties of dimensions 3 and 4 over finite fields.** The isogeny class of an abelian variety over a finite field is determined by its characteristic polynomial (i.e. the characteristic polynomial of its Frobenius endomorphism). We describe the set of characteristic polynomials which occur in dimension 3 and 4; this completes the work of Xing (we will recall his results).

The characteristic polynomial of an abelian variety of dimension $g$ defined over $\mathbb{F}_q$ is monic, with integer coefficients, of degree $2g$ and the set of its roots consists in couples of complex conjugated numbers of modulus $\sqrt{q}$. A polynomial having those properties is called a Weil polynomial. Thus every Weil polynomial has the form

$$t^{2g} + a_1 t^{2g-1} + \cdots + a_g t^g + q a_{g-1} t^{g-1} + \cdots + q^{g-1} a_1 t + q^g$$

where $a_1, \ldots, a_g \in \mathbb{Z}$. Our problem splits in two sub-problems:

1. Determine the $(a_1, \ldots, a_g)$ corresponding to Weil polynomials.
2. Given a Weil polynomial, determine if it is the characteristic polynomial of some abelian variety.

The first problem is solved by manipulations of symmetric functions. To deal with the second problem, we use Honda-Tate Theory.

**Marc Hindry: Brauer-Siegel theorems for abelian varieties over global fields.** The classical Brauer-Siegel theorem states that for a family of number fields of given degree, the product of the unit regulator by the class number behaves asymptotically like the square root of the discriminant.

We would like to show that for abelian varieties of a given dimension, defined over a fixed global field, the product of the Néron-Tate regulator by the cardinality of the Tate-Shafarevic group behaves asymptotically like the height of the abelian variety.

The statement over number fields remains essentially conjectural; the analog over function fields, though not entirely settled, is far more advanced. In particular there are specific families for which we can unconditionally prove the Brauer-Siegel statement.

A large part of the talk is joint work with Amilcar Pacheco; this research is also linked with work of Micha Tsfasman, Boris Kunyavski et Alexey Zykin.

**Masaaki Homma: Rational curves with many rational points over a finite field**. We are interested in the set of rational points of a particular curve $C$ in $\mathbb{P}^2$ over a finite field $\mathbb{F}_q$; especially in counting the number of points of this set, and in describing their configuration. Even though an $\mathbb{F}_q$-point of $\mathbb{P}^2$ is a singular point of $C$, we count it among $\mathbb{F}_q$-rational points of $C$. Hence even if the normalization of $C$ is $\mathbb{P}^1$, the number $N_q(C)$ of $\mathbb{F}_q$-points of $C$ may exceed $q+1$. However it is easy to see that under this circumstance with $\deg C = d$

$$N_q(C) \leq q + 1 + \frac{1}{2}(d-1)(d-2). \tag{1}$$

Recently, Fukasawa (Galois points for a non-reflexive plane curve of low degree, preprint, 2010) has studied a rational plane curve during his study of Galois points. This curve is given by

$$\mathbb{P}^1 \ni t \mapsto (1, t + t^q, t^{q+1}) \in \mathbb{P}^2. \tag{2}$$

This rational curve was studied originally by Ballico-Hefez (E. Ballico and A. Hefez, Nonreflexive projective curves of low degree, Manuscripta Math. 70 (1991) 385-396) in the context of nonreflexive plane curves, and they chose another representation; their model and Fukasawa's are projectively equivalent over $\mathbb{F}_{q^2}$, but not $\mathbb{F}_q$. Fukasawa's model is more interesting from a view point of finite geometry. Actually the number of $\mathbb{F}_q$-points of this model achieves the equality in (1) for $d = q + 1$.

We will dicuss codes made from the curve (2), and a generalization of (2):

$$\mathbb{P}^1 \ni t \mapsto (1, t + t^q + \cdots + t^{q^{n-1}}, t^{1+q} + \cdots + t^{q^{n-2}+q^{n-1}}, \ldots, t^{1+q+\cdots+q^{n-1}}) \in \mathbb{P}^n.$$

**Everett Howe: New results on curves of genus** 4 In this talk we present a number of new results on $N_q(4)$, the maximal number of points on a genus-4 curve over $\mathbf{F}_q$, for small values of $q$. For example, we compute the exact value of $N_q(4)$ for 13 values of $q$ less than 100 for which the value was previosly unknown. Our results depend both on lowering the known upper bounds on $N_q(4)$ and on producing curves with many points.

Analyzing some examples of genus-4 curves attaining the maximal number of points suggested an interesting explicit construction: In any characteristic other than 2 or 3, we can produce arbitrarily large sets of non-isomorphic genus-4 curves whose Jacobians are all isomorphic to one another as abelian varieties without polarization. Earlier work of Ciliberto and van der Geer showed that pairs of such curves exist, but no explicit examples were known before now.

**Kamal Khuri-Makdisi: Using algebraic values of modular forms to obtain models for modular curves**. A projective smooth curve can be described either explicitly by equations, or implicitly by giving enough points in projective space that only one curve of given genus and degree can interpolate through these points. For some applications the latter representation is more efficient. We investigate this approach on the modular curve $X(N)$, using a family of modular forms on $\Gamma(N)$ having a nice interpretation with respect to the moduli problem of elliptic curves with $N$-torsion.

**David Kohel: A normal form for elliptic curves in characteristic** 2 We construct a normal form for elliptic curves over a field of characteristic 2 equiped with a rational 4-torsion point, providing an analog of the normal form of Edwards. We provide a native construction in characteristic 2, determined by consideration of invariants forms of a permutation representation of the dihedral group $D_4$. As a side-effect, we find a second normal form analogous to the Jacobi model in $\mathbb{P}^3$. We provide a alternative construction of each family as the reduction of a 2-minimal model of the Edwards and Jacobi models, with respective level structures $\mathbb{Z}/4\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z})^2$. We remark that the basis of addition laws for the former is independent of the curve parameters, and provide strikingly simple and efficient forms for the group law.

**Aristides Kontogeorgis: Weierstrass semigroups and Galois module structure of spaces of holomorphic differentials of curves**. We will present some relations between the Weierstrass semigroup at a wild ramified point of a curve and the space of holomorphic polydifferential of curves. There will be given some applications to the deformation theory of curves with automorphisms.

**Philippe Langevin: A note on Helleseth's conjecture.** In this talk, we discuss about a conjecture proposed by Hellesseth in the framework of maximal sequences and theirs cross-correlations. In particular, we give divisibility properties on the spectra of power permutations over a finite field of characteristic two.

**Gregor Leander: A new construction of bent functions based on Z-bent functions**. Dobbertin has embedded the problem of construction of bent functions in a recursive framework by using a generalization of bent functions called Z-bent functions. Following his ideas, we generalize the construction of partial spreads bent functions to partial spreads Z-bent functions of arbitrary level. Furthermore, we show how these partial spreads Z-bent functions give rise to a new construction of (classical) bent functions. We underline the variety given by this construction by showing that all bent function in 6 variables can be constructed in this way.
This is joint work with Sugata Gangopadhyay, Anand Joshi and Rajendra Kumar Sharma.

**Elodie Leducq: Proofs of two conjectures on APN functions**. Let $q = p^n$, $p$ being a prime number, $n$ an integer.
If $f : \mathbb{F}_q \to \mathbb{F}_q$, for all $a$ and $b \in \mathbb{F}_q$, we denote by $N_f(a, b)$ the number of solutions in $\mathbb{F}_q$ of the equation $f(x + a) - f(x) = b$. We say that $f$ is APN if

$$\Delta_f = \max(N_f(a, b), a, b \in \mathbb{F}_q, a \neq 0) = 2.$$

Dobbertin, Mills, Müller, Pott and Willems have made the two following conjectures :

- For $n \geq 5$ odd, in $\mathbb{F}3^n$, the fonction $x \mapsto x^d$ is APN for

$$d = \begin{cases} \frac{3^m-1}{2} & \text{if } n \equiv 3 \mod 4 \\ \frac{3^m-1}{2} + \frac{3^n-1}{2} & \text{if } n \equiv 1 \mod 4 \end{cases}$$

- If $n$ is an odd integer, in $\mathbb{F}_{5^n}$, the fonction $x \mapsto x^d$ is APN for

$$d = \frac{5^n - 1}{4} + \frac{5^m - 1}{2}.$$

Here, we prove these two conjectures.

**Petr Lisonek: Hyperbent functions and hyperelliptic curves**. Hyperbent functions are mappings from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ with important applications in Cryptography. Let $n = 2m$. By well known results of Dillon and Carlet and Gaborit, monomial hyperbent functions can be constructed from elements $z$ in $\mathbb{F}_{2^m}$ such that

$K(z) = 0$, where $K$ is the Kloosterman sum on $\mathbb{F}_{2^m}$. Lachaud and Wolfmann related Kloosterman sum on $\mathbb{F}_{2^m}$ to a certain elliptic curve defined over $\mathbb{F}_{2^m}$.
Recently Charpin and Gong gave a construction of multinomial hyperbent functions that include Dillon's monomial functions as a special case. We show that the condition required in the Charpin and Gong construction can be expressed in terms of the number of points on certain two hyperelliptic curves.
We also give further applications of the result of Lachaud and Wolfmann quoted above. For example, we show that certain identities involving Kloosterman sums, proved from first principles in the coding theory literature, are simple consequences of isogenies between elliptic curves.

**Kit-Ho Mak: Two families of maximal curves which are not Galois subcovers of the Hermitian curve.** We show that the generalized Giulietti-Korchmaros curve (GK curve) and the maximal curve with equation $x^{q^2} - x = y^{(q^n+1)/(q+1)}$ defined over the finite field of $q^{2n}$ elements, for $n \geq 3$ odd and $q \geq 3$, are not Galois subcovers of the Hermitian curve over the same finite field. For $q = 2$, we show that the generalized GK curve is covered by the Hermitian curve.This is joint work with Iwan Duursma.

**Alina Ostafe : Algebraic Properties of Polynomial Iterations**. Partially motivated by applications to pseudorandom number generators, we discuss some (mostly open) questions about algebraic properties of polynomial dynamical systems, such as degree growth, irreducibility of iterations of polynomials, etc. In particular, we are interested in characterising the irreducible polynomials which have the property that all the iterations are also irreducible. Polynomials having this property are called *stable*. Standard heuristic, based on the density of irreducible polynomials, suggests that there should be very few stable nonlinear polynomials over finite fields while almost all polynomials over $\mathbb{Z}$ should be stable. Unfortunately questions of this type are notoriously hard, and essentially the all known results apply only to univariate quadratic polynomials.

The goals of this talk are to present:

- degree growth of iterations of polynomials/rational functions and other algebraic properties of such dynamical systems;
- the few results that are known for stable quadratic polynomials, in particular about the orbit length of such dynamical systems, which introduce to the area such new tools as the Weil bound of character sums;
- new nontrivial results about the stability of arbitrary polynomials over finite fields;
- open questions related to this problem.

*Joint work with O. Ahmadi, D. Gomez, F. Luca, A. P. Nicolás, D. Sadornil and I. E. Shparlinski*

**Ferruh Ozbudak : Certain planar functions and number of rational points of some curves**. (joint work with Gohar M. Kyureghyan and Alexander Pott) We study a class of functions over finite fields and we show that certain maps among them are planar. We also get results on the number rational points of some related curves.

**François Rodier: Highly resistant Bollean functions for cryptography**. The vector Boolean functions are used in cryptography to construct block ciphers and an important criterion on these functions is highly resistance to differential cryptanalysis. An example is given by APN functions: a function $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ is said to be *almost perfect nonlinear* (APN) on $\mathbb{F}_{2^n}$ if the number of solutions in $\mathbb{F}_{2^n}$ of the equation $f(x + a) + f(x) = b$ is at most 2, for all $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$.
So far, the study of APN functions has focused on power functions. Recently it was generalized to polynomials. On the other hand, several authors showed that APN functions did not exist in certain cases.
Hernando and McGuire showed a result on the classification of APN monomials which has been conjectured for 40 years: the only exponents such that the monomial $x^d$ are APN over infinitely many extension of $\mathbb{F}_2$

are of the form $2^i + 1$ or $4^i - 2^i + 1$. Then it is natural to formulate for polynomial functions the following conjecture.
*Conjecture (Aubry, McGuire and Rodier) :* A polynomial can be APN for an infinity of ground fields $\mathbb{F}_{2^n}$ only if it is CCZ equivalent to a monomial $x^t$ where $t$ is an exponent as before.
One means to prove this conjecture is to remark that the APN property is equivalent to the fact that the rational points of a certain algebraic surface $S(f)$ in a 3-dimensional space linked with the polynomial $f$ defining the Boolean function are all in a surface $V$ independent of $f$. When this surface is irreducible a Weil's type bound may be used to approximate the number of rational points of this surface. When it is too large the function $f$ cannot be APN. This method let us prove the conjecture in a number of cases.
We review some results which have been proved in this direction.

**Karl Rökaeus: Computer aided search for curves with many points**. The Riemann hypothesis for curves (proved by Weil) give an upper bound on how many rational points there can be on a smooth curve of genus $g$ defined over a finite field of cardinality $q$. This bound is rarely met; when $g/q$ is big it can be improved substantially and in general it is unknown how far it is from being achieved. For small $q$ (mostly powers of 2 and 3) and $g < 50$ much work has been done on constructing curves with many points, and this combined with work improving the upper bounds has now determined the maximum possible number of points on such a curve, or a small interval in which it lies. In this talk we discuss which of the established methods for proving existence of curves with many points that are suitable for computer search over bigger finite fields. For example, the zeta function of a curve can be used to prove existence of covers with many points, so by listing all curves of genus up to 2 for some finite fields we can improve upon the known lower bounds.

**Cécilia Salgado: Zariski density of rational points on del Pezzo surfaces of low degree**. Let $k$ be a non-algebraically closed field and $X$ be a surface defined over $k$. An interesting problem is to know whether the set of $k$-rational points $X(k)$ is Zariski dense in $X$. A lot of research is done in this field but, surprisingly, this problem is not completely solved for the simplest class of surfaces, the rational, where one expects a positive answer. In this lecture I will focus on del Pezzo surfaces, a important subclass of rational surfaces. I will talk about the cases already treated (mainly by Manin), as well as the two cases left open, the del Pezzo surfaces of degrees one and two, presenting recent results (in progress) in the field.

**Jean-Pierre Serre: What does the Sato-Tate conjecture mean ?**

**Tetsuji Shioda: On the $(21)_5$-configuration of curves on the supersingular K3 surface of Artin invariant 1 in characteristic 2**. The title refers to a remarkable configuration, discovered by Dolgachev and Kondo, on such a K3 which consists of two sets of 21 disjoint curves such that every curve in one set intersects exactly 5 curves in the other set. We give a simple construction of such using a linear code defined in terms of the height formula of Mordell-Weil lattices.

**Vijaykumar Singh: On Characteristic polynomial of supersingular abelian varieties over finite fields**. We give the list of characteristic polynomials of supersingular abelian varieties of dimensions up to 7, and the simple procedure to find them which can in principle be extended to all dimensions.

**Ben Smith: Naive algebraic computation of low-degree isogenies in genus 2**. Recent work of Lubicz and Robert (implemented in the AVIsogenies software package by Bisson, Cosset, and Robert) has given us an effective means of computing $(l, l)$-isogenies of abelian surfaces over finite fields. Their approach is based on theta functions, and requires a (possibly large) field extension to ensure enough theta $4l$-level structure is rational. In this talk we describe an algebraic construction, avoiding (explicit) theta functions, which allows us to rapidly compute $(3, 3)$-isogenies with at most a quadratic field extension, avoiding the bottleneck introduced by the theta structure field extensions.

**Henning Stichtenoth: On the number of rational points on algebraic curves over finite fields**. (joint work with Nurdagül Anbar, Sabancı University) For a curve $\mathcal{C}$ over a finite field $\mathbb{F}_q$ (projective, non-singular, absolutely irreducible) we denote by $g(\mathcal{C})$ (resp. $N(\mathcal{C})$) the genus (resp. the number of $\mathbb{F}_q$-rational points) of $\mathcal{C}$. The classical Hasse-Weil Theorem says that for given $q$ and $g = g(\mathcal{C})$,

$$q + 1 - 2g\sqrt{q} \leq N(\mathcal{C}) \leq q + 1 + 2g\sqrt{q} \ ,$$

i.e. $N(\mathcal{C})$ lies in a finite interval. A lot of effort has been put into improving the upper bound of this interval, partly motivated by applications of curves with 'many' points in coding theory and cryptography, but also since 'the question represents an attractive mathematical challenge' (van der Geer).

In this talk, we change the point of view slightly: we fix the finite field $\mathbb{F}_q$ and a non-negative integer $N$ and ask for all possible values of $g$ such that there exists a curve $\mathcal{C}$ over $\mathbb{F}_q$ of genus $g$,
having exactly $N$ rational points. As follows immediately from the Hasse-Weil Theorem, $g$ must satisfy the condition

$$g \geq \frac{N - (q+1)}{2\sqrt{q}} \ .$$

Our main result is

**Theorem 1.** *Given a finite field $\mathbb{F}_q$ and an integer $N \geq 0$, there is an integer $g_0 \geq 0$ such that for every $g \geq g_0$, there exists a curve $\mathcal{C}$ over $\mathbb{F}_q$ with $g(\mathcal{C}) = g$ and $N(\mathcal{C}) = N$.*

A generalization of this result is

**Theorem 2.** *Given a finite field $\mathbb{F}_q$ and non-negative integers $b_1, \ldots, b_m$. Then there exists an integer $g_1$ with the following property: for every $g \geq g_1$ there exists a curve $\mathcal{C}$ over $\mathbb{F}_q$ with $g(\mathcal{C}) = g$ such that $\mathcal{C}$ has exactly $b_r$ points of degree $r$, for $r = 1, \ldots, m$.*

Theorem 2 has a nice interpretation in terms of the $L$-polynomial (the numerator of the zeta function) of the curve $\mathcal{C}$. One can - under certain conditions - prescribe the first coefficients of the $L$-polynomial of $\mathcal{C}$ arbitrarily.

**Bianca Viray: Bounding the denominators of Igusa class polynomials using arithmetic intersection theory**. The CM methods for constructing genus 2 curves require as input a bound on the size of the denominators of the Igusa class polynomials. Moreover, a sharper bound results in a faster algorithm. We build on work of Bruinier-Yang and Yang to give a very sharp bound on the denominators, under some assumptions on the CM field and away from the 2-primary part. We will discuss how bounding the denominators is related to the problem of counting embeddings of the ring of integers of a quartic CM field into maximal orders into a division algebra, and how we use this to obtain a bound. If time permits, we will also discuss work in progress to remove the assumptions mentioned above. This is joint work with Kristin Lauter.

**Gabor Wiese: On modular Galois representations modulo prime powers.** The talk is based on joint work with Imin Chen and Ian Kiming. I will discuss different notions of modularity for Galois representations modulo prime powers, relations between them and illustrate them by some examples.

**Yuri Zarhin: Ranks of abelian varieties in towers of function fields.** We discuss explicit examples of abelian varieties of bounded rank in infinite towers of function fields of characteristic zero. In many cases we are able to compute the rank at every layer of the tower. This is a report on a joint work with Douglas Ulmer (Georgia Tech).