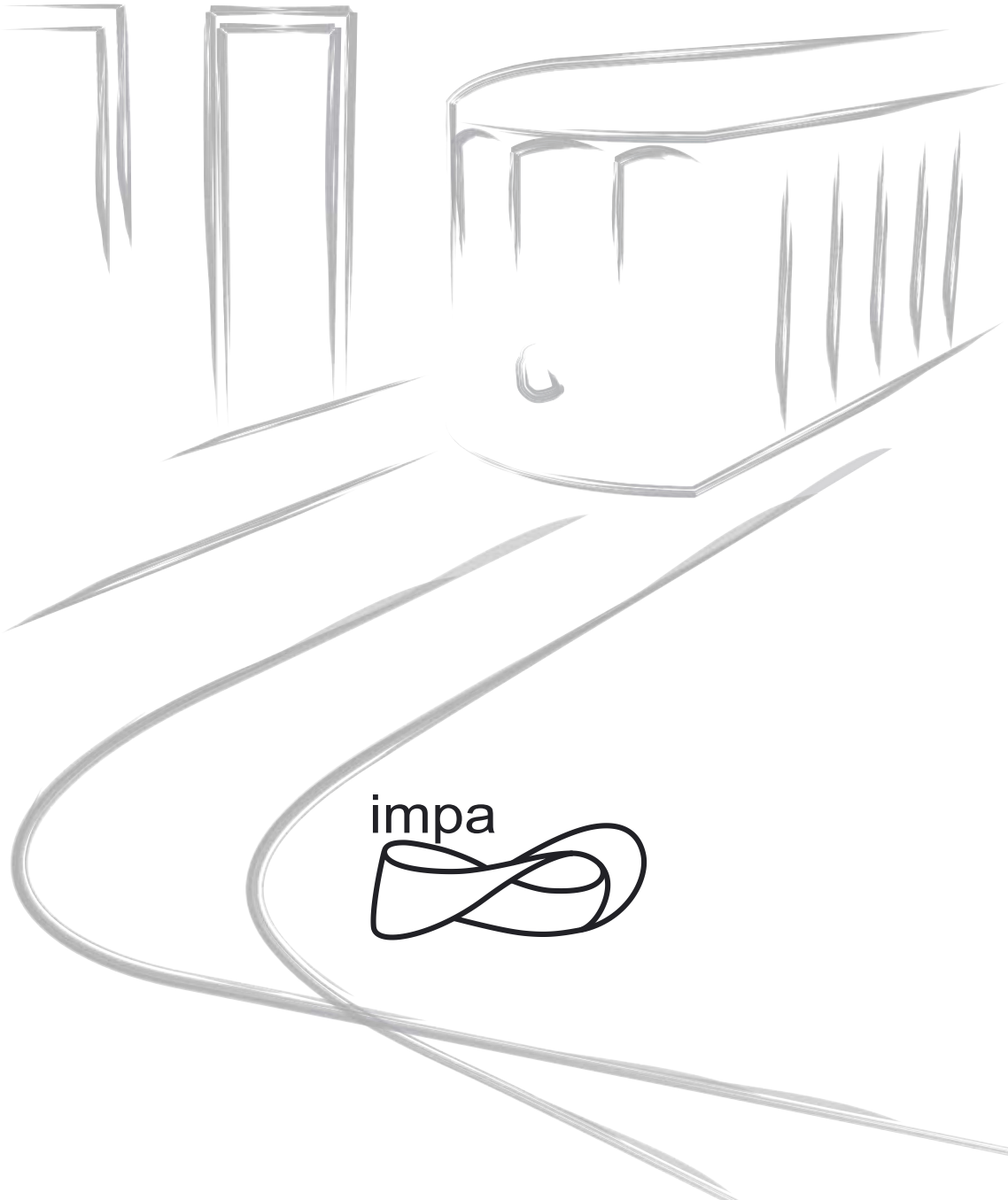
10th ALGA Meeting

Algebraic Geometry and Commutative Algebra



July 05th to 09th, 2010

IMPA, Rio de Janeiro, Brazil

sponsors

CNPq FAPERJ INCTMat

Program at a glance

Auditorium 1

Hour	Monday 5	Tuesday 6	Wednesday 7	Thursday 8	Friday 9
09:00 - 09:50	**Registration & Check in**	Felipe Voloch (Texas U., Austin, U.S.A.)	Steven Kleiman (MIT, Cambridge, U.S.A.)	**Free Morning**	Carlos D'Andrea (U. Barcelona, Spain)
10:00 - 10:10	Welcome address	**09:50 - 10:10 Coffee Break**	**09:50 - 10:10 Coffee Break**		**09:50 - 10:10 Coffee Break**
10:10 - 11:00	Arnaud Beauville (Nice, France)	Marcos Jardim (UNICAMP, Campinas, Brazil)	Marcelo Saia (USP, São Carlos, Brazil)		Hajime Kaji (Waseda U, Tokyo, Japan)
11:10 - 12:00	Henning Stichtenoth (Sabanci U., Istanbul, Turkey)	Jesse Kass (U. Michigan, Ann Arbor, U.S.A.)	Masaaki Homma (Kanagawa, Yokohama, Japan)		Arnaldo Garcia (IMPA, Rio de Janeiro, Brazil)
12:00 - 14:00	**Lunch**				
14:00 - 14:50	Aron Simis (UFPe, Recife, Brazil)	**Afternoon**	Claude Carlet (Paris 8, France)	Gabor Korchmaros (U. Basilicata, Potenza, Italy)	
15:00 - 15:50	Alicia Dickenstein (UBA, Buenos Aires, Argentina)		Sebastian Casalaina-Martin (U. Colorado, Boulder, U.S.A.)	Enrique Reyes (CINVESTAT, Mexico)	
15:50 - 16:10	**Coffee Break**		**Coffee Break**	**Coffee Break**	
16:10 - 16:35	Herivelto Borges (UNICAMP, Campinas, Brazil)		Cícero Carvalho (UFU, Uberlândia, Brazil)	Marco Pacini (UFF, Rio de Janeiro, Brazil)	
16:40 - 17:05	Thiago Fassarella (UFF, Rio de Janeiro, Brazil)		Alex Abreu (IMPA, Rio de Janeiro, Brazil)	André Contiero (UFAL, Maceió, Brazil)	
17:20	**Cocktail**				

Confirmed Speakers

Alex Abreu - IMPA, Rio de Janeiro, Brazil

Arnaud Beauville - Nice, France

Herivelto Borges - UNICAMP, Campinas, Brazil

Claude Carlet - Paris VIII, France

Cícero Carvalho - UFU, Uberlândia, Brazil

André Contiero - UFAL, Maceió, Brazil

Carlos D'Andrea - U. Barcelona, Spain

Alicia Dickenstein - UBA, Buenos Aires, Argentina

Thiago Fassarella - UFF, Rio de Janeiro, Brazil

Arnaldo Garcia - IMPA, Rio de Janeiro, Brazil

Masaaki Homma - Kanagawa, Yokohama, Japan

Marcos Jardim - UNICAMP, Campinas, Brazil

Hajime Kaji - Waseda U, Tokyo, Japan

Jesse Kass - University of Michigan

Steven Kleiman - MIT, Cambridge, U.S.A.

Gabor Korchmaros - U. Basilicata, Potenza, Italy

Sebastian Casalaina-Martin - University of Colorado at Boulder

Marco Pacini - UFF, Niterói, Brazil

Enrique Reyes - CINVESTAT, Mexico

Marcelo Saia - USP, São Carlos, Brazil

Aron Simis - UFPe, Recife, Brazil

Henning Stichtenoth - Sabanci U., Istanbul, Turkey

Felipe Voloch - Texas U., Austin, U.S.A.

Wronskians Classes on the moduli space of curves.

Alex Abreu

IMPA

Resumo/Abstract:
The purpose of this talk is to compute the class of a divisor in the moduli space of stable curves of genus 2n, defined as the closure of the locus of smooth curves C possessing a pair of points (P,Q), such that P is a special ramification point of the linear system $K_C(-nQ)$ and Q is a special ramification point of$K_C(-nP)$.

The Brauer group of Enriques and K3 surfaces

Arnaud Beauville

Universit de Nice

Resumo/Abstract:
The Brauer group is an important, but somewhat subtle, invariant of algebraic varieties. I will recall its definition, discuss a few applications, and explain how to handle it in an example, namely Enriques surfaces and their K3 covers.

Minimal value set polynomials and Frobenius non-classical curves

Herivelto Borges

ICMC-USP, São Carlos, SP.

One can easily check that for any polynomial $F \in \mathbb{F}_q[x]$ of degree $d \geq 1$, the set $V_F = \{F(\alpha) : \alpha \in \mathbb{F}_q\}$ satisfies

$$\lfloor \frac{q-1}{d} \rfloor \leq \#V_F \leq q. \tag{1}$$

Polynomials attaining the lower bound in (1) are called minimal value set polynomials (shortened to m.v.s.p.). The first results regarding the characterization of such polynomials were presented by Carlitz, Lewis, Mills and Straus in the early 1960's.

In this talk, we discuss some recent results (joint work with R.Conceição) related to the characterization of m.v.s.p. As an application, we address a construction of curves of type $F(y) = G(y)$ with many rational points, and point out a connection with q-Frobenius non-classical curves. For instance, the following characterization is obtained.

Theorem 0.1. *Let $\mathcal{C} : F(y) = G(x)$ be an irreducible curve defined over $\mathbb{F}_q$. If $\min\{\#V_F, \#V_G\} > 2$, then $\mathcal{C}$ is a q-Frobenius non-classical curve if and only if F and G are m.v.s.p. with $V_F = V_G$.*

Highly Nonlinear Filter Boolean Functions with High Algebraic Immunity for Stream Ciphers

Claude Carlet

Univ. Paris 13

Resumo/Abstract:
Boolean functions, that is, functions from the vectorspace $/F/_2^n/$ of all binary vectors of length /n/, to the finite field with two elements $/F/_2$, play a central role in the security of symmetric (i.e. conventional) cryptography. Cryptographic transformations (pseudo-random generators in stream ciphers, S-boxes in block ciphers) can be designed by appropriate composition of nonlinear Boolean functions. We shall recall how Boolean functions can be used in the pseudo-random generators of stream ciphers. We shall describe the principle of the recent algebraic attacks on them and the related notion of algebraic immunity. A first series of constructions of infinite classes of Boolean functions with optimum algebraic immunity has been proposed. All of them give functions which do not allow resistance to another kind of cryptanalysis called fast correlation attacks. We shall describe more recent infinite classes of functions which achieve an optimum algebraic immunity and allow resistance to all other attacks on stream ciphers.*

A reduced Groebner basis for the defining ideal of algebras which admit a complete set of near weights

Cícero Carvalho
Faculdade de Matemática
Universidade Federal de Uberlândia

In 1998 Høholdt, van Lint and Pellikaan introduced the concept of a "weight function" defined on a $\mathbb{F}_q$-algebra and used it to construct linear codes, obtaining among them the algebraic geometry (AG) codes supported on one point. Later, in 1999, it was proved by Matsumoto that an $\mathbb{F}_q$-algebra that admits a weight function is actually the ring of regular functions of a certain type of affine curve, and all codes produced using a weight function are actually AG codes supported on one raional point. In independent works, Miura and Pellikaan described a Groebner basis for the ideal defining those algebras. Recently, "near weight functions" (a generalization of weight functions), also defined on a $\mathbb{F}_q$-algebra, were introduced by E. Silva to study codes supported on several points and, in a recent work, Carvalho and Silva proved that R is an $\mathbb{F}_q$-algebra that admits a so-called complete set of m near weight functions if and only if R is the ring of regular functions of an affine geometrically irreducible algebraic curve defined over $\mathbb{F}_q$ whose points at infinity have a total of m rational branches; also, the codes produced using the algebra and the near weight functions are exactly the AG codes supported in several rational points. In this talk we would like to present some new results on these $\mathbb{F}_q$-algebras, in particular, we present a description of a reduced Groebner basis for their defining ideals.

Computing singularities of rational curves

Carlos D'Andrea

Universitat de Barcelona

Resumo/Abstract:
Given a birational parameterization of a curve C, a lot of information about its singularities can be extracted from simple matrices naturally arising from elimination theory (typically, Sylvester type-matrices).

In this talk we will review different methods for computing the singularities of the curves, and focus on the particular case of plane curves for which the geometry is very rich. We will describe some explicit adjoint pencils in terms of determinants and provide some generators of the Blow-up algebras associated to the parameterization of C. We will also give a complete factorization of the invariant factors of these matrices. This is a joint work with Laurent Bus.

The structure of smooth lattice polytopes with high codegree

Alicia Dickenstein

Universidad de Buenos Aires

Resumo/Abstract:
A lattice polytope P in R^n is the convex hull of a finite set of integer points. The codegree c of P is the smallest positive integer c such that the dilated polytope cP has an interior integer point. We say that P has high codegree if $c > n/2 + 1$. Following joint work with Sandra di Rocco, Benjamin Nill and Ragni Piene, we show the Cayley structure of smooth lattice polytopes with high codegree using tools from projective algebraic geometry and from combinatorics. This answers for smooth toric varieties a question by Batyrev and Nill and solves partially an adjunction-theoretic conjecture by Beltrametti-Sommese.

Developable webs

Thiago Fassarella

Universidade Federal Fluminense

Resumo/Abstract:
A germ of analytic subvariety on P^n is called developable if its Gauss map does not have maximal rank. The study of these varieties has been undertaken by algebraic/differential geometers at the beginning of the XXth century, but after a while the interest faded. The subject has been revisited by Griffiths-Harris in late 1970's and remains alive today even if with less activity than once. This talk will report on work in progress about developable codimension one k-webs on P^n, i.e. webs with all leaves developable. I will review the classification of these objects when $k = 1$ and $n < 5$ (developable foliations on $P2$, $P3$ and $P4$); and will exhibit some irreducible components of the space of k-webs on P^n having developable webs as generic member.

On constructions of towers over finite fields

Arnaldo Garcia

IMPA

Resumo/Abstract:
The subject of this talk goes around the question: How many rational points (points with coordinates in a finite field) can a nonsingular projective curve have? The answer to this question is the famous Hasse-Weil theorem. Ihara noticed the weakness of this theorem for high genus curves. We are going to use the language of function fields. A function field F over a finite field k is a finite and separable extension of the rational function field k(x), with k being algebraically closed in F. Let g(F) denote the genus and N(F) denote the number of places of degree one (rational places). We are interested in the behaviour of the ratios N(F)/g(F), when the genus is very large with respect to the cardinality of the finite field k. A tower over k is an infinite sequence of function field extensions $F_(n+1)/F_n with g(F_n)$ growing to infinity with n. We are going to present some ideas on constructions of good towers; i.e., towers with large limits for the ratios of rational places by the genus. The towers will be recursive; i.e., they will be obtained from a single polynomial in two variables with coefficients in the finite field k.

Sziklai conjecture on the number of points of a plane curve over a finite field

Masaaki HOMMA, Kanagawa University, Japan
(joint work with Seon Jeong KIM, Gyeongsang National University, Korea)

Two years ago, Peter Sziklai conjectured an upper bound for the number N of points of a plane curve over a finite field, which depends only on the degree d of the curve and the cardinality q of the finite field. Namely he conjectured inequality $N \leq (d-1)q+1$, which is stronger than Segre's inequality $N \leq (d-1)q + \lfloor \frac{d}{2} \rfloor$. But, for $d = q = 4$ there is an example against this conjecture. Recently, however, we have settled this conjecture affirmatively except for this counter-example.

ADHM variety and perverse coherent sheaves on P2

Marcos Jardim

UNICAMP, Campinas, Brazil

Resumo/Abstract:
Based on previous work by Hulek and Donaldson. Nakajima showed that there is a 1-1 correspondence between "stable" solutions of the ADHM equation and torsion-free sheaves on P2 which restrict trivially at a line. In this work, we study the properties of arbitrary solutions of the ADHM equation, relating them to perverse coherent sheaves on P2. Joint work with Renato Martins (UFMG).

Local Structure of the Theta Divisor

Jesse Kass

University of Michigan

Resumo/Abstract:
The theta divisor of a non-singular curve is a special ample divisor on its Jacobian. Its study dates back to Riemann, whose Singularity Theorem computes the multiplicity of theta at a point. Due to work of Kempf and others, today we now have a detailed understanding of the divisor. These results have been used to describe the geometry of the canonical model of smooth curves, establish the irrationality of certain threefolds, and prove the Torelli Theorem. It is natural to ask how this body of work extends to the case of singular curves.

Thanks to the work of many mathematicians, including Altman, Alexeev, Caporaso, Esteves, Kleiman, and Soucaris, a natural analogue of the theta divisor has been constructed on the compactified Jacobian of a stable curve. However, comparatively little is known about the geometry of this divisor. I will discuss some results concerning the local geometry of this theta divisor, and, in particular, I will prove a generalization of the Riemann Singularity Theorem for integral nodal curves.

This work is joint with Sebastian Casalaina-Martin.

Gauss maps in positive characteristic

Hajime KAJI

Waseda U, Tokyo, Japan

Resumo/Abstract:
his is a story of projective algebraic geometry in positive characteristic. I survey a history of studies on Gauss maps of projective varieties in positive characteristic, and state some recent results of a joint-work with S. Fukasawa and K. Furukawa. The theme of those studies is condensed to the following:

Problem (S.L.Kleiman (1987)): "It would be good to have an example of a smooth (nonreflexive) curve X such that every tangent makes 2 or more contacts or to prove that such X do not exist." [S.L.Kleiman (with A.Thorup), "Intersection theory and enumerative geometry: A decade in review," in "Algbraic Geometry – Bowdoin 1985," Proc. Symposia Pure Math. 46 (1987).]

The Epsilon Multiplicity and Equisingularity

Steve Kleiman

MIT, Cambridge

Resumo/Abstract:
The epsilon multiplicity is a new invariant of a submodule of a free module of finite rank over a Noetherian local ring. It generalizes the Samuel multiplicity of an ideal primary to the maximal ideal; it generalizes the Buchsbaum-Rim multiplicity of a submodule of finite colength. The epsilon multiplicity obeys many of the same rules as those older multiplicities, including Teissier's Principle of Specialization of Integral Dependence. Consequently, the new multiplicity yields an invariant of germs of ARBITRARY isolated complex-analytic singularities whose constancy across the members of a flat family implies its Thom-Whitney equisingularity.

ON MAXIMAL CURVES AND THEIR AUTOMORPHISM GROUPS

GÁBOR KORCHMÁROS

Abstract. Let $\mathcal{X}$ be a projective, geometrically irreducible, non-singular, algebraic curve defined over a finite field $\mathbf{F}_{q^2}$ of order q^2. If the number of $\mathbf{F}_{q^2}$-rational points of $\mathcal{X}$ satisfies the Hasse-Weil upper bound, then $\mathcal{X}$ is said to be $\mathbf{F}_{q^2}$-maximal. It has been known for a long time that the quotient curve of $\mathcal{X}$ with respect to any subgroup of the $\mathbf{F}_{q^2}$-automorphism group $Aut(\mathcal{X})$ of a $\mathbf{F}_{q^2}$-maximal curve is still an $\mathbf{F}_{q^2}$-maximal curve. This offers a wide possibility to derive new $\mathbf{F}_{q^2}$-maximal curves from a known one, and hence it gives a strong motivation for the study of $\mathbf{F}_{q^2}$-automorphism groups of an $\mathbf{F}_{q^2}$-maximal curve $\mathcal{X}$.

In this talk we survey some recent results on automorphism groups of maximal curves.

Dipartimento di Matematica, Universitá della Basilicata, Campus Universitario di Macchia Romana, 85100 Potenza, Italy

E-mail address: gabor.korchmaros@unibas.it

Simultaneous stable reduction for curves with ADE singularities

Sebastian Casalaina-Martin

University of Colorado at Boulder

Resumo/Abstract:
A basic question in moduli theory is to describe a stable reduction of a given family of curves. That is given a family of curves where the generic fiber is stable, one would like to "replace" the fibers that are not stable in such a way as to obtain a family of stable curves. Typically this will only be possible after a generically finite base change, and the question is to describe such a base change as well as the total space of the new family. The aim of this talk is to present joint work with Radu Laza where we describe stable reductions for a families of curves with ADE singularities. Time permitting, applications to the moduli space of stable curves and the Hassett-Keel program will also be discussed.

On the second Abel map for a singular curves.

Marco Pacini

Universidade Federal Fluminense

Resumo/Abstract:
The d-th Abel map of a smooth curve associates to a d-tuple of points of the curve the line bundle associated to the d points. Recently, the problem of contructing an Abel map for a singular curve has been considered by many authors. The problem has been solved if the curve is irreducible and if d=1. In this talk we will discuss some progress on the case d=2. This is a joint work with Juliana Coelho and Eduardo Esteves.

Toric Ideals of Combinatorial Structures

Enrique Reyes
CINVESTAV-IPN

Abstract

Let $H = (V, E)$ be a hypergraph, where $V = \{x_1, \ldots, x_n\}$ and $E = \{y_1, \ldots, y_m\}$ are the vertex set and the edge set respectively. The toric ideal P_H associated to H is the kernel of the homomorphism of k-algebras

$$\phi: k[y_1, \ldots, y_m] \to k[x_1, \ldots, x_n],$$

induced by $\phi(y_i) = x^{v_i}$, where v_i is the characteristic vector of y_i.

We present a characterization of the some hypergraphs whose toric ideals are complete intersections. In particular we will analyse the case of the graphs and digraphs.

A CHARACTERIZATION OF NEWTON NON DEGENERATE MODULES AND MULTIPLICITIES

M. J. SAIA, ICMC-USP, SÃO CARLOS, S.P.

Joint work with: R. Callejas-Bedregal and V. H. Jorge-Pérez

Abstract

The computation of the Samuel multiplicity of an ideal of finite co-length is one of the main tools used to calculate geometric invariants of singularities and it is a challenging problem in commutative algebra to show methods which alow us to compute such multiplicity. There are some cases where this computation is possible. When I is an ideal generated by monomials in $\mathbb{C}[[x_1, ..., x_n]]$, Teissier showed that that integral closure of this ideal is generated by the monomials $X^k = x_1^{k_1}...x_n^{k_n}$ whose exponents are in the Newton polyhedron of I. As the Samuel multiplicity depends only of the integral closure of such an ideal, the multiplicity can be computed in terms of the Newton polyhedron of I.

This result was extended by Saia which characterized the class of ideals in $\mathcal{O}_n$ with monomial integral closure. Biviá-Ausina characterizes a class of submodules M in $\mathcal{O}_n^p$ such that the integral closure of M and the Buchsbaum-Rim multiplicity are easily computable. The main characteristic of this class is that they can be written as $M = I_1 \bigoplus I_2 \bigoplus \ldots \bigoplus I_p$ where each I_j is an ideal of finite colength in $\mathcal{O}_n$. Then he showed how to characterize the Buchsbaum-Rim multiplicity of these submodules M in $\mathcal{O}_n^p$ in terms of the mixed multiplicities of the ideals I_j, as defined by Teissier.

Here we show that this characterization can be extended to a bigger class of finite co-length modules M in $\mathcal{O}_n^p$ which can be written as $M = M_1 \bigoplus \ldots \bigoplus M_s$ and each M_i is a submodule of finite co-length in $\mathcal{O}^{p_i}$ with $p_1 + \ldots + p_s = p$. We introduce a new set of multiplicities on a set of finite colength modules $M_1, \ldots, M_s$, called $\star$-multiplicities, which is appropriate to our purpose. We characterize the Buchsbaum-Rim multiplicity of such M where each M_i is a submodule of finite co-length in $\mathcal{O}^{p_i}$ with $p_1 + \ldots + p_s = p$, in terms of the $\star$-multiplicities associated to the submodules $M_1 \ldots M_s$. We show how to compute the $\star$-multiplicities of such modules in terms of appropriate Newton polyhedra, we associate the integral closure of the module M with the integral closure of the submodules M_i. Then under a Newton non-degeneracy condition for the submodules M and M_i we characterize the $\star$-multiplicities in terms of volumes of Newton polyhedra.

Departamento de Matemática, Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo - Campus de São Carlos, Caixa Postal 668, 13560-970 São Carlos, SP, Brazil

E-mail address: mjsaia@icmc.usp.br

On the number of rational points on algebraic curves over finite fields

Henning Stichtenoth, Sabancı University, Istanbul, Turkey

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. *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 $N(\mathcal{C}) = N$.*

Elements of large order in finite fields

Felipe Voloch

Texas U., Austin, U.S.A.

Resumo/Abstract:
We discuss the problem of constructing elements of multiplicative high order in finite fields of large degree over their prime field. We prove that for points on a plane curve, one of the coordinates has to have high order. We also discuss a conjecture of Poonen for subvarieties of semiabelian varieties for which our result is a weak special case. We also prove an analogue for elliptic curves.