Arithmetics, Geometry, Cryptography and Coding Theory
May 18 - 22, 2015

Nurdagül Anbar: On idempotent quadratic functions and the weight distribution of subcodes of Reed-Muller codes

(Joint work with Wilfried Meidl and Alev Topuzoğlu). The Walsh transform $\widehat{Q}$ of a quadratic function $Q : \mathbb{F}_{2^n} \to \mathbb{F}_2$ satisfies $|\widehat{Q}(b)| \in \{0, 2^{\frac{n+s}{2}}\}$ for all $b \in \mathbb{F}_{2^n}$, where $0 \leq s \leq n-1$ is an integer depending on Q. In this work, we investigate two classes of such quadratic Boolean functions which attracted a lot of research interest. For arbitrary integers n we determine the distribution of the parameter s for both of the classes, $\mathcal{C}_1 = \{Q(x) = \mathrm{Tr}(\sum_{i=1}^{\lfloor (n-1)/2 \rfloor} a_i x^{2^i+1}) \ : \ a_i \in \mathbb{F}_2\}$, and the larger class $\mathcal{C}_2$, defined for even n as $\mathcal{C}_2 = \{Q(x) = \mathrm{Tr}(\sum_{i=1}^{(n/2)-1} a_i x^{2^i+1}) + \mathrm{Tr}_{n/2}(a_{n/2} x^{2^{n/2}+1}) \ : \ a_i \in \mathbb{F}_2\}$. Our results have two main consequences. We obtain the distribution of the nonlinearity for the rotation symmetric quadratic Boolean functions, which have been attracting considerable attention recently. We also present the complete weight distribution of the corresponding subcodes of the second order Reed-Muller codes.

References

[1] Berlekamp, E.R., Sloane, N., *The weight enumerator of second-order Reed-Muller codes*, IEEE Trans. Inform. Theory IT-16, 745-751 (1970)

[2] Khoo, K., Gong, G., Stinson, D., *A new characterization of semi-bent and bent functions on finite fields*, Designs, Codes, Cryptogr. 38, 279–295 (2006)

[3] Meidl, W., Roy, S., Topuzoğlu, A., *Enumeration of quadratic functions with prescribed Walsh spectrum*, IEEE Trans. Inform. Theory 60, 6669–6680 (2014)

Christine Bachoc : An analogue of Vosper's Theorem for Extension Fields

We are interested in characterising pairs S, T of F-linear subspaces in a field extension L/F such that the linear span ST of the set of products of elements of S and of elements of T has small dimension. Our central result is a linear analogue of Vosper's Theorem, which gives the structure of vector spaces S, T in a prime extension L of a finite field F for which

$$\dim_F(ST) = \dim_F(S) + \dim_F(T) - 1,$$

when $\dim_F(S), \dim_F(T) \geq 2$ and $\dim_F(ST) \leq [L : F] - 2$. The proof involves the study of codes of quadratic forms over finite fields with respect to an unusual weight function. This is a common work with Oriol Serra and Gilles Zémor.

Régis Blache : Valuations of exponential sums, congruences for L-functions, and consequences

Let $k = \mathbb{F}_q$ denote a finite field of characteristic p, $f \in k[x_1, \ldots, x_n]$ a polynomial, and ψ a non trivial additive character of k.

For any integer $r \geq 1$, let $k_r \subset \overline{k}$ denote the degree r extension of k, and ψ_r the extension of ψ to k_r defined by $\psi_r := \psi \circ \mathrm{Tr}_{k_r/k}$. One defines an exponential sum $S_r(f)$ for each $r \geq 1$, and an L-function

$$S_r(f) := \sum_{x \in k_r^n} \psi_r(f(x)), \ L(f,T) := \exp\left(\sum_{r \geq 1} S_r(f) \frac{T^r}{r}\right).$$

Note that from the orthogonality relations on character sums, zeta functions of varieties are particular L-functions; for instance, if H is the hypersurface in $\mathbb{A}^n$ having equation $h(x_1, \ldots, x_n) = 0$, then its zeta function can be rewritten $Z(H, qT) = L(yh, T)$.

We are interested in some p-adic properties of these objects, following Stickleberger, Chevalley, Warning, Ax, Katz and others. Precisely, we look for the lowest p-adic valuations of their reciprocal roots or poles; this is often encoded as the first segment of a Newton polygon, which will be our main object of study.

We shall first consider the first slope. We give a sharp lower bound for the q-adic valuations of exponential sums in the one dimensional case, determining

$$\min\{v_q(S(f)),\ f \in k[x],\ \deg f = d\}.$$

Then we describe a congruence for L-functions "along the first slope of their Newton polygon", and list some of its consequences

(i) about the first vertex of the Newton polygon of (the numerator of the zeta function of) an Artin-Schreier curve, and the non- existence of supersingular such curves for certain genera;

(ii) about the zeta function of varieties having their number of points divisible by p (for instance a degree d hypersurface in $\mathbb{A}^n$ with $n > d$); in this case the congruence leads to some generalisation of the Hasse-Witt (or Cartier-Manin) matrix.

Irene Bow: Computing L-functions of superelliptic curves

Let Y be a superelliptic curve defined over a number field, i.e. Y is a cyclic cover of the projective line. In this talk I report on algorithmic results for computing the local L-factor and the conductor exponent of Y at the primes of bad reduction. The key ingredient is the calculation of the stable reduction of Y at the bad primes. As an application, we verify the functional equation numerically for a large class of examples. In particular, we consider a class of hyperelliptic curves of genus $g \geq 2$ defined over $\mathbf{Q}$ which have semistable reduction everywhere. This is joint work with Stefan Wewers and Michel Börner.

Alain Couvreur: An upper bound on the number of points of a projective variety and a proof of a conjecture of Ghorpade and Lachaud

For an arbitrary closed subset X of a projective space $\mathbf{P}^n$ over a finite field, we provide an upper bound on its number of rational points depending only on the dimension n of the ambient space, the dimensions of the irreducible components of X and their embedding degrees in $\mathbf{P}^n$.

This bound generalizes in some sense Serre's bound on the number of points of a hypersurface and is proved by using several combinatorial lemmas based on double counting arguments. In the equidimensional case, the bound turns out to be sharp and provides a proof of a conjecture due to Gorpade and Lachaud.

Agnès David: Of Kisin varieties and Galois deformation rings

Kisin varieties are some Grassmannians introduced to study the modularity of Galois representations. I will present a combinatorial object encoding the structure of these varieties. It enables us to describe, algorithmically and theoretically, their points over finite fields and their geometric and topological properties. I will then explain the consequences of these results for certain Galois deformation rings. This is work in progress with X. Caruso and

A. Mézard.

Florent Demeslay: Class formula in positive characteristic

In 2012, Taelman prove a formula for a certain value of Goss L-function which is an analogue for function fields in positive characteristic of the class number formula. We extend this result and we obtain a similar formula for two other kinds of L-functions. We try to show the analogy with the number field case through the talk.

Ernst-Ulrich Gekeler: Algebraic curves with many rational points over non-prime finite fields

We construct curves over finite fields with properties similar to those of classical elliptic or Drinfeld modular curves (as far as elliptic points, cusps, ramification, ... are concerned), but whose coverings have Galois groups of type $\mathbf{GL}(r)$ over finite rings ($r \geq 3$) instead of $\mathbf{GL}(2)$. In the case where the finite field is non-prime, there results an abundance of series or towers with a large ratio "number of rational points/genus". The construction relies on higher-rank Drinfeld modular varieties and the supersingular trick and uses mainly rigid-analytic techniques.

Sudhir Ghorpade: Tsfasman-Boguslavsky Conjecture for Polynomial Systems and Generalized Hamming Weights of Projective Reed-Muller Codes

In the late 1980's, Tsfasman conjectured an optimal bound on the number of points of a projective hypersurface in $\mathbb{P}^m$ of degree d over the finite field $\mathbb{F}_q$ with q elements. This was soon proved by J.-P. Serre and independently by A. B. Sørensen in 1991. More generally, for a system of r linearly independent homogeneous polynomials in $m+1$ variables of degree d with coefficients in $\mathbb{F}_q$, there is an elaborate conjecture of Tsfasman and Boguslavsky that proposes an optimal bound for the number of common zeros in $\mathbb{P}^m(\mathbb{F}_q)$ of this system. The case $r = 1$ corresponds to the above result of Serre and Sørrensen. The conjecture is proved in the affirmative when $r = 2$ and $d < q - 1$ by Boguslavsky in 1997. The general case appears to have been open although an affine analogue was proved in the context of coding theory by Heijnen and Pellikaan in 1998.

We prove that the conjecture holds in the affirmative for any $r \leq m + 1$ and $d < q - 1$. Further, we show that the conjecture is false, in general. More precisely, using the work of Zanella (1998), we show that when $d = 2$, the conjecture is false for at least $\binom{m-1}{2}$ values of positive integers r with $m + 1 < r \leq \binom{m+2}{2}$.

These results are intimately related to the determination of the generalized Hamming weights of projective Reed-Muller codes, and as such we make some progress in the problem of explicit determination of these generalized Hamming weights.

This is a joint work with Mrinmoy Datta.

References

[1] M. Boguslavsky, On the number of solutions of polynomial systems, *Finite Fields Appl.* **3** (1997), 287–299.

[2] A. Couvreur, An upper bound on the number of rational points of arbitrary projective varieties over finite fields, `arXiv:1409.7544 [math.AG]`, 2014.

[3] M. Datta and S. R. Ghorpade, On a conjecture of Tsfasman and an inequality of Serre for the number of points on hypersurfaces over finite fields, `arXiv:1503.03049 [math.AG]`.

[4] P. Heijnen and R. Pellikaan, Generalized Hamming weights of q-ary Reed-Muller codes, *IEEE Trans. Inform. Theory* **44** (1998), 181–196.

[5] J.-P. Serre, Lettre à M. Tsfasman, Journées Arithmétiques (Luminy, 1989). *Astérisque* No. 198-200 (1991), 351–353.

[6] A. B. Sørensen, Projective Reed-Muller codes, *IEEE Trans. Inform. Theory* **37** (1991), 1567–1576.

Aurore Guillevic: Computing Discrete logarithms in GF(p^n): Practical Improvement of the Individual Logarithm Step

This talk will focus on the last step of the number field sive algorithm used to compute discrete logarithms in finite fields. We consider here non-prime finite fields of very small extension degree: $1 \leq n \leq 6$. These cases are interesting in pairing-based cryptography: the pairing output is an element in such a finite field. The discrete logarithm in that finite field must be hard enough to prevent from attacks in a given time (e.g. 10 years). Within the CATREL project we aim to compute DL records in finite fields of moderate size (e.g. in GF(p^n) of global size from 600 to 800 bits) to estimate more tightly the hardness of DL in fields of cryptographic size (2048 bits at the moment). The best algorithm known to compute discrete logarithms in large finite fields (with small n) is the number field sieve (NFS):

(1) polynomial selection: select two distinct polynomials f, g defining two number fields, such that they share modulo p an irreducible degree n factor, and have additional properties to improve the next two steps.
(2) sieving: sieve over elements that satisfy relations, to build the *factor basis* made of prime ideals of small norm.
(3) linear algebra: compute the kernel of a large matrix computed the step before. Then the logarithm of each element in the factor basis is known.
(4) individual logarithm: for a given element $s \in \mathrm{GF}(p^n)$, decompose it over the factor basis to finally compute its discrete logarithm.

The most time consuming steps are the second and third: sieving and linear algerbra. After the sieve and the linear algebra, the logarithms of the prime ideals of small norm are known. To finally compute the discrete logarithm of the given element s, we lift s in one of the number fields and factor it in prime ideals as with "small" elements in the sieve step. However here, s does not have a small norm (bounded by $B \ll Q$). Its norm is very large, in particular, larger than Q. The usual way is to test for many $s' = s \cdot g^e$ with g the given generator of GF(p^n) until the norm of s' is smooth enough. The time spent to find a good e is asymptotically less than the sieving time. In practice, another modification of s' is computed to reduce its norm. In [JLSV06], the authors write $s' = a(x)/b(x)$ with a, b of coefficients of size $\sim p^{1/2}$ instead of p. With $n = 4$ the norm of s is $O(p^{11/2})$. Their method compute a, b of norm $O(p^{7/2})$. One need to factor into small prime ideals two elements a, b instead of one s'.

for our record computations of discrete logarithms in $\mathbb{F}_{p^n}$ with $2 \leqslant n \leqslant 6$, we improve the preparation of s, so that its norm in the number field is less than Q. This improves its smoothness property. Assume that we want to compute the discrete logarithm of s in the larger subgroup of prime order ℓ of GF(p^n), with $\ell \mid \Phi_n(p)$. We decompose s in $\varepsilon \cdot s'$ with ε in a subfield or in a subgroup of order prime to ℓ and s' with reduced coefficient size. We still have $\log_g s = \log_g s' \bmod \ell$. We use a tower representation of GF(p^n) with subfields for our purpose. We reduce the norm of $s \in \mathbb{F}_{p^4}$ from $O(p^{11/2})$ to $O(p^{7/2})$, $s \in \mathrm{GF}(p^3)$ from $O(p^6)$ to $O(p^2)$ and $s \in \mathbb{F}_{p^2}$ from $O(p^4)$ to $O(p)$. This does not change the asymptotic complexity of this last step but this improves a lot its running time for small n.

References

[JLSV06] A. Joux, R. Lercier, N. Smart, and F. Vercauteren. The number field sieve in the medium prime case. In *Advances in Cryptology–CRYPTO 2006*, volume 4117 of *Lecture Notes in Comput. Sci.*, pages 326–344. Springer, 2006.

Emmanuel Hallouin : Weil bounds of higher orders (joint work with Marc Perret

We describe an euclidean process which permits to recover easily the Weil and Ihara bounds on the number of points on cuvres over finite fields. We show how this process leads to new bounds.

Masaaki Homma : An analogue of a theorem of Tallini on plane curves over finite fields

More than a half century ago, G. Tallini (Rend. Mat. e Appl. (5) 20 (1961) 431–479) studied the irreducible plane curves of minimum degree containing all $\mathbb{F}_q$-points of $\mathbb{P}^2$. Several years ago, we revived his work as follows (with S. J. Kim, Linear Algebra and its Applications 438 (2013) 969-985):

Theorem .

- *Let C be an irreducible curve of degree d in $\mathbb{P}^2$ defined over $\mathbb{F}_q$. If $C(\mathbb{F}_q) = \mathbb{P}^2(\mathbb{F}_q)$, then $d \geq q+2$.*
- *Moreover, if $d = q+2$, the equation of C can be written as*

$$(*) \qquad (Y^qZ - YZ^q, Z^qX - ZX^q, X^qY - XY^q)A \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = 0$$

  where A is a 3×3-matrix over $\mathbb{F}_q$.
- *Let C_A be a plane curve defined by* $(*)$, then obviously $C(\mathbb{F}_q) = \mathbb{P}^2(\mathbb{F}_q)$ and the following conditions are equivalent:
  (i) C_A is irreducible;
  (ii) C_A is nonsingular;
  (iii) the characteristic polynomial of A is irreducible over $\mathbb{F}_q$.

Now we handle a similar phenomenon, in which we replace the condition $C(\mathbb{F}_q) = \mathbb{P}^2(\mathbb{F}_q)$ by supposing $C(\mathbb{F}_q) = \mathbb{A}^2(\mathbb{F}_q)$.

Everett Howe: Polarizations on $E \times E$ and genus-4 curves with many points

We present an algorithm that, given an odd prime power q, will produce in time roughly $q^{3/4}$ a genus-4 curve over $\mathbf{F}_q$ with small defect. Heuristically, we expect that when q is large enough the curve produced will have defect at most 4. The analysis of the algorithm depends on understanding the category of principal polarizations on an abelian surface of the form $E \times E$, where E is an elliptic curve with CM by a maximal order. We reinterpret results of Hayashida from the 1960s to show that this category is equivalent to the category of left ideals in a certain quaternion algebra.

Annamaria Iezzi: Towards maximal singular curves over finite fields

We present a construction of singular curves over finite fields with many rational points and relatively small arithmetic genus. This construction enables us to prove some results on the maximum number of rational points on an absolutely irreducible projective algebraic curve defined over $\mathbb{F}_q$ of geometric genus g and arithmetic genus π. We end up providing some results and properties of maximal singular curves. This is a joint work with Yves Aubry.

Antoine Joux : A simplified setting for discrete logarithms in small characteristic finite fields

The hardness of computing discrete logarithms in finite field has served as a foundation for many public key cryptosystems. In the last two years, tremendous progress have been made in the case of small characteristic finite fields.

In this talk, we present a simplified description of the algorithmic framework that has been developed to solve this problem faster. This framework is an index calculus approach that relies on two main ingredients, the definition of the extension field and the generation of multiplicative relations in this field. Given a base field $\mathbb{F}_q$, we construct its extension field $\mathbb{F}_{q^k}$ in the following way: we find two polynomials of low degree h_0 and h_1 with coefficients in $\mathbb{F}_q$ such that $x^q h_1(x) - h_0(x)$ has an irreducible factor of degree k over $\mathbb{F}_q$.

To generate relations, we start from the well-known identity:

$$X^q - X = \prod_{c \in \mathbb{F}_q} (X - c).$$

Combining substitution of X by a fraction in the identity with the field definition, we easily obtain many multiplicative relations. This is enough to obtain the logarithms of a factor base of small degree elements in polynomial time.

Once this is done, we use a descent procedure to recursively express any element of the finite field $\mathbb{F}_q$ into elements represented by polynomials of lower degree. This procedure is quite complex but ultimately leads to a quasi-polynomial time algorithm for the discrete logarithm problem in small characteristic finite fields.

The simplified description presented in this talk is a joint work with Cécile Pierrot and also improves the complexity of the polynomial time pre-computation.

Grigory Kabatiansky: On double sparse compressed sensing via coding theory and its different applications

The Compressed Sensing (CS) problem is to reconstruct an n-dimensional t-sparse vector $x \in \mathbb{R}^n$ by a few linear measurements $s_i = (h_i, x)$ even if measurements (h_i, x) are known with some errors e_i, i.e. the goal of CS is to find a t-sparse solution x of the following equation

$$s = Hx^T + e, \tag{1}$$

if Euclidean length $||e||_2$ of the error vector e is small enough, see [1],[2].

We introduced in [3] a particular case of this problem when both vectors x and e are sparse, which we called double-sparse CS problem. In [3] our motivation was based on discrete version of CS problem. Later we have found solutions for discrete version of CS problem [4] and for double-sparse CS problem in its original continuous form [5]. Note, that the discrete version of CS problem is closely related to the famous Ulam's problem "search with a lie" [6]. Recently we have found a new application and a new statement of the problem motivated by coding for adder channel with noise [7].

Our main result in all these statements of the problem is the explicit construction of a family of optimal matrices (i.e. "codes"), which have the number of rows (code's redundancy) equals to $2(t+l)$, where l is the sparsity of the error vector e. Moreover we propose for these matrices a very simple algorithm how to recover x.

References

[1] D.L. Donoho, "Compressed sensing", IEEE Transactions on Information Theory, v. 52 (4), pp. 1289-1306, 2006.

[2] E.J. Candes, T. Tao, "Near-Optimal Signal Recovery From Random Projections: Universal Encoding Strategies?", IEEE Transactions on Information Theory, v. 52 (12), pp. 5406 - 5425, 2006.

[3] G.Kabatiansky, S.Vladuts, "What to do if syndromes are corrupte also", in Proc. Int.Workshop Optimal Codes, Albena, Bulgaria, 2013.

[4] G.Kabatiansky, V.Lomakov, S.Vladuts, "On error correction in presence of noise in channel and syndrom", Problems of Information Transmission, 2015 (in print).

[5] G.Kabatiansky, C.Tavernier, " Double sparse compressed sensing problem", in Proc. ACCT-2014, Svetlogorsk, Russia, pp. 181-185, 2014.

[6] S.M.Ulam. "Adventures of a Mathematician". Scribner's, New York, 1976.

[7] S.C.Chang and E.J.Weldon, "Coding for T-user multiple access channels", IEEE Trans. Inform. Theory, v. 25 (6), pp. 684-691, 1979.

Kamal Khuri-Makdisi: Bounding Brill-Noether loci over finite fields, with applications to Jacobian arithmetic For a smooth projective curve C of genus g over the finite field F_q, the behavior of a typical effective divisor of degree d can be used to describe slightly faster Jacobian group arithmetic than my previous work based on linear algebra on spaces of sections. To know how often a divisor is typical, one needs to bound the number of points on a Brill-Noether locus of special divisors with prescribed h^0. I will present a result along these lines that allows one to show that the fraction of typical divisors is at least $1-k/q$, where k is an effective constant that depends (sadly, exponentially) only on the genus g. This means that for very large finite fields, one can compute with a high probability of success using only typical divisors.

David Kohel: On extremal traces and RM in genus 2 We interpret the Sato-Tate distributions of USp(4) and SU(2)^2 in terms of a stratification of the moduli space $\mathcal{M}_2$ of genus 2 curves by Humbert surfaces $\mathcal{H}_D$, parametrizing real multiplication by a real quadratic subring of End(J) of discriminant D. As a consequence we derive explicit heuristics for the relative preponderance of curves with RM among curves $C/\mathbf{F}_q$ of genus 2 with extremal trace of Frobenius.

This is joint work with Gilles Lachaud and Yih-Dar Shieh.

Gilles Lachaud : On the Number of Points of Algebraic Sets over Finite Fields

We determine upper bounds on the number of rational points of an affine or projective algebraic set defined over an extension of a finite field by a system of polynomial equations, including the case of an algebraic set not defined over the base field. A special attention is given to irreducible but not absolutely irreducible algebraic sets, which satisfy smaller bounds. We study the case of complete intersections, for which we give a decomposition, coarser than the decomposition in irreducible components, but more directly related to the polynomials defining the given algebraic set. We describe families of algebraic sets having the maximum number of rational points in the affine case, and a large number of points in the projective case.

These results will be put in perspective with the inequalities recently proved by Alain Couvreur on one side, and those of Mrinmoy Datta and Sudhir Ghorpade on the other side. arXiv:1405.3027

Kristin Lauter : A new hard problem? (Ring) Learning With Errors

In the last 5 years, there has been rapid growth of ?lattice-based? cryptography, largely because of encryption systems which have been proposed based on the hardness of the new Learning With Errors (LWE) problem and its Ring variant (RLWE). These systems have generated a lot of excitement and attention because they include solutions for homomorphic encryption, which allows for example for outsourcing of computation on encrypted data. Despite many generic security reductions which have been proved, new work shows that the Ring Learning With Errors problem may not be hard in general, for the ring of integers in general number fields. In this talk we will survey some of the known reductions and attacks, and paint a picture of the current expected security of these systems for certain choices of number rings, i.e. cyclotomic number rings. (Based on joint work with Kirsten Eisentraeger, Sean Hallgren, Yara Elias, Ekin Ozman, Kate Stange)

Reynald Lercier : Covariant algebra of the binary nonic and the binary decimic

A famous result by Hilbert (1890) states that the algebra of invariants for a linear reductive group is finite. For the action of $SL_2(C)$ on binary forms, the result was already known since Gordan (1868). Many (heavy) calculations have been done at this time to compute these algebras, but after few decades, it became clear that it was hopeless to deal by hand with forms of degree > 8.

One century later, we might think that with the help of computers it is possible to go further on the subject. But, despite some recent new computations made for forms of degree 7 or 8 (Croeni,Bedratyuk), no new results had been obtained about covariant bases for a single binary form.

In this talk, we start form Gordan's algorithm and present some improvements that decrease significantly its complexity. As a result, we have applied the method to forms of degree 9 and 10, and have been able to prove after one day of computations that the covariant algebras conjectured by Brouwer et al. (see `http://www.win.tue.nl/ aeb/math/invar.html`) are indeed complete.

(Joint work with Marc Olive)

Bernard Le Stum: An introduction to rigid cohomology

Counting points requires sophisticated tools and Rigid cohomology provides one. We will consider very explicit elementary examples, show the power of cohomological methods in general and work out the explicit case of rigid cohomology. More precisely, we will use de Rham technics and see how the overconvergence conditions naturally appear when Frobenius enters the show.

Christian Maire: On the Class groups in an unramified p-tower.

In this talk, I will discuss asymptotic properties of the p-Class group in unramified p-towers. I will introduce a new constant and will present some observations/questions mixing number theory and group theory. It is a joint work with Pr. Hajir (UMASS).

Irene Marquez Corbella : Structural Cryptanalysis of McEliece schemes with Algebraic Geometry Codes
This talk is based on joint works with A. Couvreur (INRIA Saclay - GRACE Project) and R. Pellikaan (Eindhoven University of Technology).

Code-based Cryptography together with lattice-based cryptography, multivariate cryptography and hash-based cryptography are the principal available techniques for Post-quantum cryptography. McEliece proposed the first cryptosystem based on the theory of error correcting codes in 1978. The principle of code-based cryptography is based on the following one-way trapdoor function: it is easy and fast to encode a message using linear transformation; but the general decoding problem was proven to be NP-complete in 1978 for the Hamming metric. Decoding is also believed to be hard for a quantum computer. The trapdoor information is that there exists families of codes that have efficient decoding algorithms.

McEliece proposed to use binary Goppa codes. But several proposals based on other families of algebraic codes appeared in the literature. For instance, Generalized Reed-Solomon codes, subcodes of them and Binary Reed-Muller codes. All of these shemes are subject to polynomial or sub-exponential time attacks.

Another attempt, suggested by Janwa and Moreno was to introduce Algebraic Geometry codes. This scheme was broken for codes on curves of genus $g \leq 2$ by Faurer and Minder. However this attack has several drawbacks which makes it impossible to extend to higher genera. In this talk we present a general attack against this proposal based on square code considerations, that is the component wise product of codewords. The point is that evaluation codes do not behave like random codes with respect to the star product *"the square of Algebraic Geometry codes has smaller dimension than that of the square of a random code of the same dimension"*.

The attack presented in this talk consist in pushing this argument forward in orther to compute a filtration of the public code by a family of very particular subcodes. This filtration methods yields to an Error Correcting Pair of the public code in $\mathcal{O}(n^4)$ operations in $\mathbb{F}_q$ where n denotes the code length. This Error-Correcting Pair allows to decrypt any encrypted message in $\mathcal{O}(n^3)$ operations. This alternative attack has been implemented in Magma and broke for instance a $[729, 404]$ 126–error correcting Hermitian code (with genus 36) over $\mathbb{F}_{81}$ (which had 182-bits security with respect to ISD attacks)in 21 minutes. Using an Intel ® CoreTM 2 Duo 2.8 GHz.

Guillermo Matera : Estimates on the number of rational points of singular complete intersections over a finite field and applications

We shall discuss a new explicit version of the Hooley-Katz estimate on the number of rational points of a singular projective complete intersection defined over a finite field. Our approach relies on tools of classical algebraic geometry. In particular, a crucial ingredient is a new effective version of the Bertini smoothness theorem for singular complete intersections. We shall also comment on applications of our results to two classical combinatorial problems over a finite field: estimates on the average value set and the distribution of factorization patterns of families of univariate polynomials.

Tohru Nakashima: AG codes from restriction of vector bundles to divisors

We introduce certain nonlinear codes defined by restriction of a vector bundle to a family of divisors on a smooth projective variety defined over a finite field. This is a higher dimensional generalization of the code introduced by Savin in the case of curves. We give estimates for the parameters under the weak stability condition on the bundles and consider some examples in the case of rational surfaces.

Nhut Nguyen: Some developments on towers over cubic finite fields

Recently, new explicit towers of function fields over all non-prime finite fields have been introduced by Bassa, Beelen, Garcia and Stichtenoth [BBGS15]. They give lower bounds for the Ihara constant $A(q)$ for all non-prime q. For cubic q's, their lower bound for $A(q)$ meets the bound obtained by the explicit tower of Bezzera, Garcia and Stichtenoth [BGS05]. While the genus of each of the function fields in Bezzera et al.'s tower was completely determined, there are just bounds on the genera in Bassa et al.'s ones. In this talk, we show that one of towers of Bassa et al. is a subtower of Bezzera et al.'s and use this relationship to compute the genus of every function field in Bassa et al.'s tower. We also determine its exact limit, using the results from [Bee04].

References

[BBGS15] A. Bassa, P. Beelen, A. Garcia, and H. Stichtenoth. Towers of Function Fields over Non-prime Finite Fields. *Moscow Mathematical Journal*, 15(1):1–29, 2015.

[Bee04] P. Beelen. Graphs and recursively defined towers of function fields. *Journal of Number Theory*, 108(2):217–240, 2004.

[BGS05] J. Bezerra, A. Garcia, and H. Stichtenoth. An explicit tower of function fields over cubic finite fields and zink's lower bound. *Journal für die reine und angewandte Mathematik*, 589:159–199, 2005.

Johan Nielsen: Power Decoding of Hermitian One-Point Codes in Sub-Quadratic Time

Algebraic geometry (AG) codes have excellent designed minimum distance, and we also know of reasonably fast algorithms for decoding them. However, the gap down to the quasi-linear complexity of decoding Reed-Solomon codes is still large.

Hermitian one-point codes is an interesting sub-family of AG codes with many properties that simplify dealing with them. The fastest, previously known decoding algorithm had a quadratic dependence on the code length.

We show how to go below quadratic complexity by building the decoder around the problem of finding a short vector in an $F[x]$-module, and performing this step using state-of-the-art algorithms from computer algebra. This approach follows recent trends in decoding of Reed-Solomon codes. Furthermore, our decoder is a "Power decoder", probabilistically capable of decoding errors beyond half-the-minimum distance for low-rate codes.
The resulting decoder has complexity $O(n^{(5/3)}M(ell))$, where n is the code length and ell is the "powering" degree parameter for the decoder. $M(m)$ denotes the field-operation complexity of multiplying two $m \times m$ matrices together over the field.

Joint work with Peter Beelen, Technical University of Denmark

Ozman Ekin: Bad Reduction of Genus Three Curves with Complex Multiplication

Let C be a smooth, absolutely irreducible genus 3 curve over a number field M. Suppose that the Jacobian of C has complex multiplication by a sextic CM-field K. Suppose further that K contains no imaginary quadratic subfield. We give a bound on the primes $\mathfrak{p}$ of M such that the stable reduction of C at $\mathfrak{p}$ contains three irreducible components of genus 1. This is joint work with Bouw, Cooley, Lauter, Garcia, Manes and Newton.

Marc Perret : Graph based strategy to exhibit good recursive towers
(Joint work with Emmanuel Hallouin)

We describe a way to find good recursive towers based over graph theory. Despite the fact that this method do not lead, up to now, to a new good tower, we think that this method is a step toward a better understanding of recursive towers. We also give a functional characterization of sets of places splitting totally in a recursive tower.

Alena Pirutka : Algebraic cycles on varieties over finite fields
Let X be a projective variety over a field k. Chow groups are defined as the quotient of a free group generated by irreducible subvarieties (of fixed dimension) by some equivalence relation (called *rational equivalence*). These groups carry many information on X but are in general very difficult to study. On the other hand, one can associate to X several cohomology groups which are "linear" objects and hence are rather simple to understand. One then construct maps called "cycle class maps" from Chow groups to several cohomological theories.

In this talk, we focus on the case of a variety X over a finite field. In this case, Tate conjecture claims the surjectivity of the cycle class map with rational coefficients; this conjecture is still widely open. In case of integral coefficients, we speak about the *integral version of the conjecture* and we know several counterexamples for the surjectivity. In this talk, we present a survey of some well-known results on this subject and discuss other properties of algebraic cycles which are either proved or expected to be true. We also discuss several involved methods.

Christophe Ritzenthaler : A new proof of a Thomae like-formula for non hyperelliptic genus 3 curves

We will discuss Weber's formula to compute the quotient of two Thetanullwerte for a plane smooth quartic in terms of the bitangents. In particular, we show how this formula can easily be derived from the Riemann-Jacobi formula.
Joint work with Enric Nart.

Yieh-Dar Shieh: Character theory and Sato-Tate groups

We demonstrate the utility of using the character theory of compact Lie groups to identify the expected Sato-Tate group of a given curve. Using this approach, we find precise invariants to derive information about the Sato-Tate group, using a smaller set of primes compared to computing the higher moments of the trace. This method is expected to be effective for curves of higher genus and curves in other families.

Jeroen Sijsling : Branches and descent

Let k be a field and let X be a curve over the algebraic closure of k of genus g with automorphism group G. Suppose that X is isomorphic with all its Galois conjugates. Is it then possible to find a curve X_0 defined over k that is isomorphic with X (over the algebraic closure)? Moreover, if one is given such an X for which the response is affirmative, can one construct X_0 and the isomorphism with X explicitly?

In general, the answer to this question is no, which is somewhat surprising. For curves of genus 2, Mestre has described the descent obstruction, and given algorithms to descend explicitly if the obstruction vanishes.

In this talk, we will describe a geometric interpretation of results of Debes and Emsalem which gives an explicit approach to the descent of more general curves. We show that the answer to the question above becomes positive if X is provided with a marked point P (possibly with non-trivial stabilizer) that is preserved by the isomorphisms between X and its conjugates. This can occasionally be used to give an explicit solution to the original descent problem.

After presenting the geometric notion of branches of a morphism, which turns out to give a clean and conceptual solution to the problem, we present some explicit calculations for plane curves, and some applications to Belyi maps. This is joint work together with John Voight.

Benjamin Smith: Slightly more practical quantum factoring through number theory

We use elementary results in number theory to investigate the number of trials needed by Shor's algorithm to factor an integer. In particular, we show that one application of Shor's order-finding algorithm is enough to factor strong RSA keys, and further, that in this case Shor's algorithm can be made completely deterministic. This implies the somewhat surprising result that while strong RSA moduli are considered the hardest case for classical factoring algorithms, they are in fact the easiest case for Shor's quantum factoring algorithm.

This is a progress report on joint work with François Morain, Thomas Lawson, and Frédéric Grosshans.

Peter Stevenhagen: Adelic points of elliptic curves

The point group of an elliptic curve E over a number field K is a finitely generated abelian group, and the distribution of the isomorphism type of this group for varying E and fixed K is largely unknown, due to our insufficient control of the rank of this group. We show that the group of adelic points of E, i.e. the group of points of E over the adele ring of K, is a topological group that is easier to describe, in terms of the Galois representation of E. More precisely, we prove that for "almost all" elliptic curves over K the adelic point group of E is a universal topological group depending only on the degree of the number field K. Nevertheless, there exist infinitely many pairwise non-isomorphic elliptic curves over K that have an adelic point group that is NOT isomorphic to this universal group. This is joint work with my student Angelakis.

Claudio Stirpe: New results on Class Number One Problem for Function Fields

In this talk we give a complete classification of function fields with class number one and we explain the role of pointless curves in this result. This is a joint work with Pietro Mercuri.

Marco Streng: Generators of the group of modularunits for $\Gamma^1(N)$ over Q

The modular curve $Y^1(N)$ parametrises pairs (E, P), where E is an elliptic curve and P is a point of order N on E, up to isomorphism. A *unit* on the affine curve $Y^1(N)$ is a holomorphic function that is nowhere zero and I will mention some applications of the group of units in the talk.

The main result is a way of generating generators (sic) of this group using a recurrence relation. The generators are essentially the defining equations of $Y^1(N)$ for $n < (N+3)/2$. This result proves a conjecture of Maarten Derickx and Mark van Hoeij.

Andrew Sutherland : Computing the image of Galois representations attached to elliptic curves

Let E be an elliptic curve over a number field K. For each integer $n > 1$ the action of the absolute Galois group $G_K := \mathrm{Gal}(\overline{K}/K)$ on the n-torsion subgroup $E[n]$ induces a Galois representation $\rho_{E,n}\colon G_K \to \mathrm{Aut}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. The representations $\rho_{E,n}$ form a compatible system, and after taking inverse limits one obtains an adelic representation $\rho_E\colon G_K \to \mathrm{GL}_2(\hat{\mathbb{Z}})$. If E/K does not have CM, then Serre's open image theorem implies that the image of ρ_E has finite index in $\mathrm{GL}_2(\hat{\mathbb{Z}})$; in particular, $\rho_{E,\ell}$ is surjective for all but finitely many primes ℓ.

I will present an algorithm that, given an elliptic curve E/K without CM, determines the image of $\rho_{E,\ell}$ in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ up to local conjugacy for every prime ℓ for which $\rho_{E,\ell}$ is non-surjective. Assuming the generalized Riemann hypothesis, the algorithm runs in time that is polynomial in the bit-size of the coefficients of an integral Weierstrass model for E. I will then describe a probabilistic algorithm that uses this information to compute the index of ρ_E in $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

Seher Tutdere : On the Torsion-Limit for Algebraic Function Fields

In this talk, we first discuss an asymptotic quantity, namely the torsion-limit, for algebraic function fields over finite fields introduced in [1, 2]. Then we give some new bounds for the torsion limit of certain towers of function fields over finite fields. Furthermore, using some bounds on the torsion limits, we will give some recent results regarding the construction of arithmetic secret sharing schemes.

This is a joint work with Osmanbey Uzunkol.

References

[1] Cascudo, I., Cramer, R., and Xing, C.: The Torsion-Limit for Algebraic Function Fields and Its Application to Arithmetic Secret Sharing, Springer CRYPTO 2011, 685–705 (2011).

[2] Cascudo, I., Cramer, R., and Xing, C.: Torsion limits and Riemann-Roch systems for function fields and applications. IEEE Transactions on Information Theory, 60(7): 3871–3888, DOI: 10.1109/TIT.2014.2314099 (2012).

Florent Ulpat-Rovetta: Construction of genus two curve starting from their invariants in characteristic 5.

In this talk, an overview will be given of the construction of genus two curve in characteristic different from 5. we split the cases according to the reduced automorphism group is trivial (generic case) or not. for the generic case, we use MestreÕs method. For the cases with more automorphisms we use ad hoc constructions. But in the generic case of characteristic 5, there are several problems and we cannot directly use MestreÕs method. We will explain how to get around these issues and give some details about the construction. Joint work with Christophe Ritzenthaler and Reynald Lercier."

Vanessa Vitse: Field extensions and index calculus on algebraic curves

Discrete logarithm index calculus algorithms are usually more efficient for non-hyperelliptic curves (Diem) than for hyperelliptic curves (Gaudry). When the field of definition is not prime, this can be taken advantage of with Nagao's algorithm, which on the contrary is more efficient for hyperelliptic curves. In this talk, we will explain why it is not possible to take into account both the field extension and the non-hyperellipticity, and why the asymptotic complexity of Nagao's algorithm is optimal using the known decomposition techniques.

Serge Vladuts : Locally recoverable codes on algebraic curves

A code over a finite alphabet is called locally recoverable (LRC code) if every symbol in the encoding is a function of a small number (at most r) other symbols. A family of linear LRC codes that generalize the classic construction of Reed-Solomon codes was constructed in a recent paper by I. Tamo and A. Barg (*IEEE Trans. Inform. Theory*, vol. 60, no. 8, 2014, pp. 4661-4676). In this talk we extend this construction to codes on algebraic curves. We give a general construction of LRC codes on curves and compute some examples, including asymptotically good families of codes derived from the Garcia-Stichtenoth towers which exceed the corresponding Gilbert-Varshamov type bound for certain range of parameters. The local recovery procedure is performed by polynomial interpolation over r coordinates of the code vector. We also obtain a family of Hermitian codes with two disjoint recovering sets for every symbol of the codeword. Based on a common work with I. Tamo and A. Barg.