Mathematisches Forschungsinstitut Oberwolfach

Report No. 1 / 2001

Finite Fields: Theory and Applications

January 7th – January 14th, 2001

The second conference on finite fields at the Mathematisches Forschungsinstitut Oberwolfach was arranged by Igor Shparlinski and Joachim von zur Gathen. Since the second organizer was absent due to illness, Igor Shparlinski did the management at Oberwolfach. He arranged the schedule, which is reprinted on the following pages, in agreement with the participants. Beside the European Union (22 attendants) and North America (16), the participants came from Russia (3), Australia (2) and Brazil, China, Turkey and Hungary (1 at a time).

There were a total of 39 presentations, covering a wide range of topics. As announced by the title of the meeting, there were talks giving new theoretical results as well as presentations of applications and experimental results. While the talks in the morning dealt with general topics on finite fields, the afternoon sessions were organized as special sessions attended to the following applications of finite fields:

- algorithms and arithmetics,
- coding theory,
- cryptography,
- exponential sums,
- finite geometry.

The talks initiated intensive discussions between the participants. Wednesday afternoon had been a planed social event. There was a walking-tour along the Wolfbach. The last session on Friday afternoon closed with a problem session where open problems had been presented.

Schedule of the meeting

Monday

General session (Chair: John Friedlander)

9:45 – 10:30	*Hendrik W. Lenstra, Jr.:* Factoring polynomials over special finite fields
10:40 – 11:25	*Winnie Li:* Eigenvalues of Ramanujan graphs and Sato-Tate conjecture
11:35 – 12:20	*Maxim Skriganov:* Coding theory, uniform distributions and related topics

Specialized session: Finite geometries, codes & function fields
(Chair: Henning Stichtenoth)

15:30 – 16:10	*James W.P. Hirschfeld:* The Desarguesian plane of order thirteen
16:15 – 16:45	*Hiren Maharaj:* On some asymptotic results in coding theory
17:00 – 17:40	*Jürgen Bierbrauer:* Codes, caps and nets
17:45 – 18:25	*Everett Howe:* Families of curves of genus two with isomorphic simple Jacobians

Tuesday

General session (Chair: Alf van der Poorten)

9:00 – 9:20	*Hendrik W. Lenstra, Jr.:* On a problem of Stichtenoth
9:25 – 9:45	*Gary L. Mullen:* Value sets of polynomials over finite fields
9:50 – 10:20	*Michael Zieve:* A new family of exceptional polynomials

General session (Chair: Hendrik Lenstra)

10:40 – 11:25	*Jose Felipe Voloch:* Beyond the Carlitz-Uchiyama bound
11:35 – 12:20	*Arnaldo Garcia:* On Tame Towers of function fields and the Drinfeld-Vladut bound

Specialized session: Algorithms I (Chair: Erich Kaltofen)

15:30 – 16:00	*Shuhong Gao:* Factoring polynomials via PDE
16:05 – 16:35	*Alan Lauder:* Factoring multivariate polynomials
16:40 – 17:10	*Michael Nöcker:* Data structures for parallel exponentiation in finite fields

Specialized session: Algorithms II (Chair: Edlyn Teske)

17:25 – 17:55	*Tom Berry:* Generalizations of continued fractions in function fields
18:00 – 18:30	*Erich Kaltofen:* On the complexity of computing determinants

Wednesday

General session (Chair: Hugh Montgomery)

9:00 – 9:45 *Michael Fried:* Exceptional covers and Davenport pairs

9:55 – 10:40 *Alfred J. van der Poorten:* Reduction mod p of the continued fraction of certain algebraic power series

10:50 – 11:35 *Edlyn Teske:* Computations in hyperelliptic function fields

11:45 – 12:25 *Phong Nguyen:* Solving low-degree polynomial equations: Lattice attacks on RSA

Thursday

General session (Chair: Winnie Li)

9:00 – 9:40 *Siguna Müller:* On the rank of appearance of Lucas sequences

9:50 – 10:30 *Francesco Pappalardi & Claudia Malvenuto:* Galois properties connected to the enumeration of permutation polynomials

General session (Chair: Aart Blokhuis)

10:40 – 11:25 *Marek Karpinski:* Polynomial time approximability of the dense Nearest Codeword Problem over finite fields

11:35 – 12:20 *Tanja Lange:* Fast arithmetic on hyperelliptic Koblitz curves for cryptography

Specialized session: Discrete logarithms & cryptography (Chair: Everett Howe)

15:30 – 16:00 *Hans Dobbertin:* Permutation polynomials and applications in geometry and cryptography

16:05 – 16:40 *Daniel Panario:* Pairs of coprime m-smooth polynomials over finite fields and the Waterloo algorithm for the discrete logarithm problem

16:45 – 17:15 *Sergey Konyagin:* Linear complexity of the discrete logarithm

Exponential sums (Chair: Gary Mullen)

17:30 – 17:55 *Zhiyong Zheng:* On a problem of H. Cohn for character sums

18:00 – 18:30 *Igor E. Shparlinski:* Exponential sums and lattices

Friday

General session (Chair: James Hirschfeld)

9:00 – 9:25 *John Friedlander:* On Diffie–Hellman triples with sparse exponents

9:30 – 9:55 *Aart Blokhuis:* On the prime power conjecture for a certain class of projective planes

10:05 – 10:45 *Stephane Ballet:* Quasi-optimal algorithms for multiplication in the extensions of $\mathbb{F}_{16}$ of degree 13, 14 and 15

10:55 – 11:35 *Lancelot Pecquet:* Reconstruction of geometric functions and applications

11:45 – 12:25 *Preda Mihăilescu:* Factoring cyclotomic polynomials over finite fields by radicals

Specialized session: Miscellaneous (Chair: Jose Felipe Voloch)

15:30 – 16:00	*Tamás Szőnyi:* Lacunary polynomials
16:05 – 16:30	*Hugh Montgomery:* Greedy sums of distinct squares
16:45 – 17:30	*Preda Mihăilescu:* Classgroup relations, the Stickelberger ideal and Catalan's conjecture
17:35 – 17:55	*Ferukh Ozbudakh:* A note on the divisor class groups of degree zero of algebraic function fields over finite fields
18:00 – 18:30	Problem session

Abstracts

Quasi-optimal algorithms for multiplication in the extensions of $\mathbb{F}_{16}$ of degree 13, 14 and 15

Stephane Ballet

From an interpolation method on algebraic curves, due to D.V. Chudnovsky and G.V. Chudnovsky, we construct effective bilinear algorithms for multiplication in the extensions of $\mathbb{F}_{16}$ of degree $13 \leq n \leq 15$, with a bilinear complexity equal to $2n+1$. These algorithms which are the first hyperelliptic algorithms of multiplication, are obtained from the hyperelliptic curve of genus 2 with plane equation $y^2 + y = x^5$.

Generalizations of continued fractions in function fields

Tom G. Berry

The classical continued fraction algorithm provides an efficient way of calculating the fundamental unit and regulator in real quadratic fields and "real" hyperelliptic function fields (those with two points at infinity). Possible generalizations are:

1. To an algorithm that calculates torsion of more general divisors of degree zero. (Observe that the regulator of a real hyperelliptic function field is the torsion of $\infty^+ - \infty^-$, where ∞^+, ∞^- are the two points at infinity).
2. To algorithms for computing fundamental systems of units in non-hyperelliptic function fields, c.f. algorithms of Voronoi, Jacobi-Perron, and more recently J. Buchmann (number fields), Hellegouarch, Paysan-le-Roux, and Scheidler-Stein (function fields).

I describe an algorithm for 1. in hyperelliptic fields, whose basic, very simple, idea extends to 2. The idea is to find iteratively a sequence of functions $f_n \in \mathbf{L}(D_n)$, where the D_n are a sequence of non-effective divisors of degree g, the genus. (In the classical continued fraction algorithm $D_n = -n\infty^+ + (n+g)\infty^-$.) Fundamental units and their analogues in 1. appear in the sequence $\{f_n\}$. In practice, one calculates not the f_n but the quotients f_n/f_{n-1}.

Codes, caps and nets

Jürgen Bierbrauer

We start by sketching a simplified approach to the theory of *cyclic codes*, which is based on the action of the Galois group. This approach generalizes to the case of *additive* codes (linearity is assumed only with respect to a subfield of the alphabet). As an interesting class of examples we study the additive generalization of *Kasami codes.* Applications of our theory include *quantum codes* and codes used for deep space communication.

Caps in Galois spaces are sets of points such that no three are on a line. We construct a family of *cyclic caps*, generalizing a construction by Ebert, Metsch and Szőnyi (joint work with A. Cassidente and Y. Edel) and study the question of completeness.

We prove bounds on caps in affine spaces, which simplify, generalize and strengthen a result of Meshulam (joint work with Y. Edel). The classification of the affine section of the *Hill up* as the unique 45-cap in $AG(5,3)$ is sketched.

A new idea due to Y. Edel, related to a classical product construction, yields new large caps in ternary affine spaces as well as an improvement upon an asymptotic result by Calderbark-Fishburn.

Finally we give an introduction to *Rosenblom-Tsfasman space* from a coding theory point of view. Construction X (lengthening) and a version of the Gilbert-Vershamov bound are generalized form Hamming space to RT-space.

On the prime power conjecture for a certain class of projective planes

Aart Blokhuis

(joint work with Dieter Jungnickel and Bernhard Schmidt)

In 1967 Dembowski and Piper showed that there are only three types of planes of order n with abelian groups of order n^2. These are translation planes, their duals, and so-called *type (b) planes.*

A classical result of André says that for (dual) translation planes this group is elementary abelian (and hence n is a prime power). Ganley showed (1976) that for type (b) planes of even order n is a prime power. We complete his result by showing the same for odd n:

Let G be an abelian collineation group of order n^2 of a projective plane of oder n. Then n is a prime power and the p-rank of G is at least $b + 1$ if $n = p^b$ for an odd prime p.

Permutation polynomials and applications in geometry and cryptography

Hans Dobbertin

We present simple examples of applications of the "multivariate" method to confirm that certain classes of "uniformly" defined polynomials are permutation polynomials. This technique has a large variety of applications in different areas like finite geometry, coding theory, cryptography etc. The necessary computations are rather complicated, but can be managed easily with Computer Algebra Packages as for instance MAGMA.

Exceptional covers and Davenport pairs

Michael Fried

This introduces a project for determining *Chow motives* from *Weil vectors.* Weil vectors refers to coefficients of a Poincaré series (like zeta functions). A fuller version of the talk is at www.math.uci.edu/∼mfried/psfiles/obwffin01-22-2001.html. *Exceptional covers* and *Davenport pairs* illustrate relations among Weil vectors.

Mature tools for the general program: *Galois stratification* from M. Fried, Solving diophantine problems over all residue class fields of a number field ... , *Annals Math.* **104** (1976), 203–233 and Fried-Jarden, Field Arithmetic, *Springer Ergebnisse II* **Vol 11** (1986) Chaps. 24-26; and rings of *Chow Motives* by Manin, and Gillet-Soulé. The Denef-Loeser paper, Definable sets, motives and p-adic integrals, to appear in the Journal of the AMS, shows cooperation between these tools.

Consider your favorite equation: $F(\mathbf{u}, z) = 0$. Use $\bar{\mathbb{F}}_q$ for an algebraic closure of the finite field $\mathbb{F}_q$. Suppose you like to count numbers of solutions $N_{q,t}$ over $\mathbb{F}_{q^t}$, for all t. You might count solutions $\bar{N}_{q,t,n}$, over $W_{q,t}/p^n$, that lift to the Witt vectors $W_{q,t}$ of $\mathbb{F}_{q^t}$. This gives sets $\mathbf{N}_{q,F} = \{N_{q,t}\}_{t=1}^{\infty}$ and $\bar{\mathbf{N}}_{q,t,n} = \{\bar{N}_{q,t,n}\}_{1 \le t, 1 \le n}$. This drives the Denef-Loeser paper. We concentrate on one finite field $\mathbb{F}_q$.

You often substitute for z to consider $F(\mathbf{u}, h(x)) = 0$: $h(x) = z$, with h a polynomial or rational function. Now we make an assumption on pairs of such substitutions from different h and g. Suppose for $t \in \chi = \chi_{h,g}$ and for each $z \in \mathbb{F}_{q^t}$,

$$(*) \qquad h(x) - z = 0 \text{ has the same number of solutions as does } g(y) - z = 0$$

Then $N_{q,t}(F(\mathbf{u},h)) = N_{q,t}(F(\mathbf{u},g))$ for $t \in \chi$. Let $\chi_{F(\mathbf{u},h),F(\mathbf{u},g)}$ be the set of t where they are equal. Then, $\chi_{F(\mathbf{u},h),F(\mathbf{u},g)} \supset \chi_{h,g}$. We'd like to put structure in the counting sets $\mathbf{N}_{q,F}$, etc. so relations as these get automatic recognition. The emphasis is that such relations among Weil vectors don't depend on your choice of *favorite equation*. We analyze relations like $(*)$ by considering $\chi_{h,g}$ with savvy.

Use $\mathbf{V}_h(L)$ for the range of the polynomial h on the field L. Let $\chi_{h,g}$ be the characteristic set $\{t \mid \mathbf{V}_h(\mathbb{F}_{q^t}) = \mathbf{V}_g(\mathbb{F}_{q^t})\}$. Don't assume $(*)$ holds. Call (h,g) a S(trong) D(avenport) P(air) if $\chi_{h,g} = \mathbb{N}^+$. Call it a DP if $\chi_{h,g}$ is infinite. Recall: $h \in \mathbb{F}_q[x]$ is *exceptional* if $h : \mathbb{F}_{q^t} \to \mathbb{F}_{q^t}$ is one-one for infinitely many t. Denote this set of exceptional t by E_h.

Suppose (h,g) is a DP and h_1 and g_1 are exceptional. The expression $h(h_1)$ denotes the composition of h and h_1. Then, $\chi_{h(h_1),g(g_1)}$ contains $E_{h_1} \cap E_{h_2} \cap \chi_{h,g}$. You have to know something about $E_{h_1}, E_{h_2}, \chi_{h,g}$ to say their intersection is infinite. The Main Theorem of the talk has a corollary saying $E_{h_1} \cap E_{h_2} \cap \chi_{h,g}$ is automatically infinite if *indecomposable* h has degree prime to p.

This is an example result from a work with W. Aitkin and L. Holt, titled *Davenport Pairs over finite fields* (preprint near completion).

Two papers (at www.math.uci.edu/∼mfried/#math) provide history and tools for considering SDPs: The definition field of function fields and a problem in the reducibility of polynomials . . . , *Ill. J. Math.* **17**, (1973), 128–146; Variables Separated Polynomials and Moduli Spaces, No. Theory in Progress, eds. K. Gyory, H. Iwaniec, J. Urbanowicz, 1997 Zakopane, Walter de Gruyter, Berlin-New York (Feb. 1999), 169–228. The controlling factor in distinguishing these with the results with Aitken-Holt is considering DPs instead of SDPs.

On Diffie-Hellman triples with sparse exponents

John Friedlander
(joint work with Igor Shparlinski)

We describe recent work joint with Igor Shparlinski to appear in SIAM J. Discrete Math. Let p be a prime with $2^n < p < 2^{n+1}$. Let W_k denote the set of n-bit integers having exactly k non-zero digits in their binary expansion. For g a primitive root modulo p consider the set of Diffie-Hellman triples $(\frac{g^x}{p}, \frac{g^y}{p}, \frac{g^{xy}}{p})$, normalized to lie in the unit cube. We are interested in trying to show that these triples, taken as x, y run through W_k, are uniformly distributed in the unit cube in the sense of H. Weyl. By symmetry we may assume that $k \le \frac{1}{2}n$.

Theorem: *Provided that $\frac{1}{2}n \ge k \ge .35n$, the above triples are uniformly distributed.*

Actually the constant .35 can be replaced by .349 . . . which arises as the zero of a certain transcendental function.

Such "sparse" exponents are of interest because for these the computation of g^x, g^y, g^{xy}, is faster than for arbitrary x and y. In the latter case, that is as x, y run through all exponents, a similar but quantitatively stronger uniformity has recently (Israel J. Math. (2000)) been obtained by R. Canetti, J. Friedlander, M. Larsen, D. Lieman, S. Konyagin and I. Shparlinski. The main lemma of that paper, a new bound for an exponential sum involving the triples, is one of the principal ingredients here as well.

Factoring polynomials via PDE

Shuhong Gao

A new method is presented for factorization of bivariate polynomials over an arbitrary field. It is based on a simple partial differential equation that gives a system of linear equations. Like Berlekamp's and Niederreiter's algorithms for factoring univariate polynomials, the dimension of the solution space of the linear system is equal to the number of absolutely irreducible factors of the polynomial to be factored and any basis for the solution space gives a complete factorization by computing gcd and by factoring univariate polynomials over the ground field. The new method finds absolute and rational factorizations simultaneously and is easy to implement for finite fields, local fields, number fields, and the complex number field. The theory of the new method allows an effective Hilbert irreducibility theorem, thus an efficient reduction of polynomials from multivariate to bivariate.

On Tame Towers of function fields and the Drinfeld-Vladut bound

Arnaldo Garcia

Let $E/\mathbb{F}_\ell$ denote a function field over $\mathbb{F}_\ell$, $N(E)$ its number of $\mathbb{F}_\ell$-rational places and $g(E)$ its genus. Let $N_\ell(g) = \max\{N(E)\colon E \text{ a function field with g(E)=g}\}$ and $A(\ell) = \limsup_{g\to\infty} \frac{N_\ell(g)}{g} \leq \sqrt{\ell} - 1$ (the last inequality being the so-called Drinfeld-Vladut bound). The aim of this talk was to present 3 towers of function fields over $\mathbb{F}_\ell$, with $\ell = p^2$ and p an odd prime, having limit equal to $p-1$ (i.e., attaining the Drinfeld-Vladut bound). Those 3 towers ξ_i $(i = 1, 2, 3)$ are recursively given by the equations $y^2 = \varphi_i(x)$ with

$$\varphi_1(x) = \frac{(x+3)^2}{8(x+1)}, \quad \varphi_2(x) = \frac{(x+1)^2}{4x} \quad \text{and} \quad \varphi_3(x) = \frac{x^2+1}{2x}.$$

The main ingredients here are the following two new properties of Deuring's polynomial $H(Z)$ describing supersingular elliptic curves in Legendre's form:

1. All roots of $H(Z)$ are 4-th powers in $\mathbb{F}_{p^2}$.
2. (Polynomial identity) $H(Z^4) = Z^{p-1} \cdot H\left(\left(\frac{Z^2+1}{2Z}\right)^2\right)$.

It was also given an explicit description of the coordinates of the supersingular points for the modular curves $X_0(2^n)$.

The Desarguesian plane of order thirteen

J.W.P. Hirschfeld

(joint work with M. Giulietti and G. Korchmáros)

The algebraic curve associated to an arc in $PG(2, q)$, with q odd, is examined using both properties of the curve itself as well as properties of the arc. The key case of $(q-1)$-arcs means that the behaviour of the associated sextic curves needs to be studied. The case of $PG(2, 13)$ is examined in detail. Noether's theorem leads to a geometric bijection between 12-arcs and their duals. The dual 12-arcs lead to optimal plane sextic curves, that is, with the maximum number of points; the 12-arcs lead to sextics whose set of rational points make them 'look like' quartics and which in contrast have very few points.

Families of curves of genus two with isomorphic simple Jacobians

Everett W. Howe

We present two pairs $(y^2 - f(x,t), y^2 - g(x,t))$ of elements of $\mathbb{Z}[t,x,y]$ with the following properties:

1. Each of the polynomials $y^2 - f(x,t)$ and $y^2 - g(x,t)$ defines a curve of genus 2 over $\mathbb{Q}(t)$.
2. If t_0 is an element of a field K such that that $y^2 - f(x,t_0)$ and $y^2 - g(x,t_0)$ define curves C and D of genus 2, then C and D are geometrically non-isomorphic, but their Jacobians are isomorphic over K (as abelian varieties without polarization).

The first pair is quite easy to write down, but the associated Jacobians are always reducible. The second pair is slightly more difficult to write down, but "generically" the Jacobians are simple. This means that for every field K there are only countably many values of t_0 that give rise to reducible Jacobians. In practice, however, we find that even over finite fields most values of t_0 lead to absolutely simple Jacobians.

On the complexity of computing determinants

Erich Kaltofen

(joint work with Gilles Villard)

We consider the bit complexity for computing a determinant of an $n \times n$ matrix with integer entries whose maximum number of bits we denote by l. Since the determinant can have as many as $(nl)^{1+o(1)}$ digits, the classical Chinese remainder approach requires $(n^4 l)^{1+o(1)}$ bit operations using classical matrix multiplication. The exponent 4 of n reduces to 3.38 when employing fast matrix multiplication. We present an algorithm that improves the exponent 4 of n to 3+1/3 using only classical matrix and integer arithmetic, and to 2.81 using fast matrix and integer arithmetic. Our algorithm combines Coppersmith's blocked Wiedemann method, now run on a dense matrix, with a baby steps/giant steps approach for evaluating the sequence of matrix moments. When applying our techniques to a 1992 result of mine, we also obtain an algorithm for computing the determinant of an $n \times n$ matrix over an arbitrary commutative ring with $O(n^{2.698})$ ring additions, subtractions, and multiplications.

Polynomial time approximability of the dense Nearest Codeword Problem over finite fields

Marek Karpinski

We design a *polynomial time approximation scheme* (PTAS) for the dense instances of *Nearest Codeword Problem* (NCP) over arbitrary finite fields. The problem can be formulated as a *linear feasibility* problem of constructing an assignment $x \in GF[q]^n$ for a given system of linear equations over $GF[q]$, which minimizes the number of unsatisfied equations. The Dense NCP was known to be NP-hard in an exact setting. The general problem is known to have exceedingly high lower approximation bound of $n^{\Omega(1)/\log\log n}$ (Dinur, Kindler, Raz, Safra, 2000), and an existence of a PTAS on dense instances comes as a surprise. The technique of solution depends on a method of approximating Smooth Polynomial Integer Programs (Arora, Karger and Karpinski, 1995), and a new density sampler technique for graphs and k-uniform hypergraphs developed recently by Bazgan, Fernandez de la Vega and Karpinski, 2000. Despite an importance of the general NCP problem, and its many applications, not much is known about "good" approximation ratio algorithms, better than of order n, and this for arbitrary fields. A challenging problem remains a design of a polynomial time approximation algorithm working on general instances of NCP within approximation ratio of $o(n)$.

Linear complexity of the discrete logarithm

Sergei Konyagin
(joint work with Igor Shparlinski)

This is our joint paper with Igor Shparlinski. We find lower bounds for the linear complexity of the discrete logarithm modulo p or modulo $p-1$ on a segment of length H. They have the order $H^{2/3}/\log p$ and $H/\log p$, correspondingly.

Fast arithmetic on hyperelliptic Koblitz curves for cryptography

Tanja Lange

We introduce a special class of hyperelliptic curves called Koblitz curves. These are curves over a finite field $\mathbb{F}_{q^n}$, q a small prime power, which are already defined over $\mathbb{F}_q$. These curves turn out to be a large source of groups suitable for cryptography. The main operation in for example the Diffie-Hellman key-exchange is the computation of m times a group element. One of the big advantages of these curves is that they allow to speed up this step. We explain how the Frobenius automorphism is used and give details on the involved algorithms. The second advantage is that the computation of the group order of the Jacobians is extremely fast for these curves whereas in the general case this is a hard problem. We establish bounds for the performance of the algorithms and give numerical evidence for them. Furthermore we provide several examples of curves suitable for cryptography.

Factoring multivariate polynomials

Alan Lauder

Given a polynomial in n variables over a field one may associate with it a convex polytope in n-dimensional real space called its Newton polytope. This is done so that if the polynomial factors then the Newton polytope decomposes, in the sense of the Minkowski sum, into the Newton polytopes of the factors. I will describe a heuristic absolute irreducibility testing method for multivariate polynomials based upon this idea, and also a factorization method for bivariate polynomials. The former algorithm has been implemented and shown to be of some practical interest, although work remains to be done on the latter.

Factoring polynomials over special finite fields

H.W. Lenstra, Jr.

I discussed the following theorem, which was obtained jointly with E. Bach and J. von zur Gathen (Finite Fields and their Applications, Volume 7, Number 1, January 2001, p. 5–28).

Theorem: *There is a deterministic algorithm that for some $c > 0$ has the following property. Given a prime p, positive integers n and k, an explicit model for $\mathbb{F}_{p^n}$, and $f \in \mathbb{F}_{p^n}[x]$, $f \neq 0$, the algorithm factors f into irreducible factors over $\mathbb{F}_{p^n}$, and if suitable generalized Riemann hypotheses are valid then it does so in time at most* $(s + \deg f +$

$n \log p)^c$, where s is the largest prime factor of $\Phi_k(p)$; here $\Phi_k(p)$ denotes the k-th cyclotomic polynomial.

In the case $k = 1$, where $\Phi_k(p) = p - 1$, this was previously known; it was done by controlling the multiplicative group $\mathbb{F}_p^\times$. For general k, one uses the group $\mathbb{F}_{p^k}^\times / \prod_{d|k,d<k} \mathbb{F}_{p^d}^\times$, which is cyclic of order $\Phi_k(p)$ and embeds in $\mathbb{F}_{p^k}^\times$ by sending the coset of α to α^m, where $m = \prod_{\ell|k,\ell\,\mathrm{prime}}(1 - p^{k/\ell})$.

On a problem of Stichtenoth

H.W. Lenstra, Jr.

Theorem: *Let p be a prime number. Then there does not exist a pair consisting of a polynomial $f \in \mathbb{F}_p[x]$ and an integer $m \in \mathbb{Z}$ such that*

1. $1 < m|p-1$;
2. $\deg f = m$, *and the leading coefficient of f is an m-th power in* $\mathbb{F}_p^\times$;
3. $0 < \mathrm{ord}_x f < m$;
4. *there is a finite set $S \subset \bar{\mathbb{F}}_p$ with $0 \in S$ and* $\{\alpha \in \bar{\mathbb{F}}_p | \exists \beta \in S \colon f(\alpha) = \beta^m\} \subset S$.

This result implies that a certain method due to Garcia, Stichtenoth, and Thomas (FFtA, 1997) for constructing "good towers of function fields" does not work over prime fields. The problem is raised whether a similar negative result holds for a wider class of construction methods.

Eigenvalues of Ramanujan graphs and Sato-Tate conjecture

Wen-Ching Winnie Li
(joint work with Ching-Li Chai)

Sato-Tate conjecture concerns the distribution of the (properly normalized) Fourier coefficients of an automorphic form for $GL(2)$ over a global field whose L-function has an Euler product. In this talk we take the ground field to be a function field K with the field of constants being a finite field F with odd characteristic, and give three families of automorphic forms for $GL(2)$ over K satisfying the Sato-Tate conjecture. The Fourier coefficients of the three families are certain character sums, arising as eigenvalues of certain Ramanujan graphs, known as norm graphs and Terras graphs. The fact that these eigenvalues are Fourier coefficients of automorphic forms was proved in my earlier work. Using geometric method, we identify such automorphic forms and verify the Sato-Tate conjecture.

On some asymptotic results in coding theory

Hiren Maharaj
(joint work with H. Niederreiter)

We demonstrate an asymptotic result in coding theory using a variant of the Goppa-construction of AG codes.

Factoring cyclotomic polynomials over finite fields by radicals

Preda Mihăilescu

Factorization of polynomials over finite fields $\mathbb{F}_q$ (q prime) can be done efficiently by improvements of Berlekamp's method due to Kaltofen, Shoup and von zur Gathen. When the polynomial to factor $\Phi_p(x)$ is cyclotomic, we show that the classic approach of factoring with radicals leads to an algorithm which requires several non power remainders in small extensions and produces the factors of $\Phi_p(x)$ by means exponentiations in "small" extensions of $\mathbb{F}_q$. Concretely, the degrees of these extensions are divisors of $\varphi(\ell)$, where $\ell | h$, the splitting index of q in the $p-$th cyclotomic field, are maximal prime powers. This reduces practically the complexity, compared to Berlekamp variants, in which exponentiations in extensions of degree $p-1$ are required. Although the asymptotic complexity is improved by factors of the order of $\log p$, in practice, for large p, the improvement is sensible. The purpose of this presentation is not only to provide an efficient factorization method for a very special purpose, but also to suggest that the use of known Galois actions can always be profitable for algorithmic purposes.

Classgroup relations, the Stickelberger ideal and Catalan's conjecture

Preda Mihăilescu

Catalan's conjecture states that the diophantine equation

$$x^U - y^V = 1$$

has no other non-trivial integer solution except $3^2 - 2^3 = 1$. The equation can be reduced to

$$(*) \qquad x^p - y^q = \epsilon,$$

with prime p, q, positive integer x, y and $\epsilon = \pm 1$. We present a last year's result which states that if $(*)$ has a solution, then $p^{q-1} \equiv 1 \bmod p^2$ and $q^{p-1} \equiv 1 \bmod p^2$. This result is under press, has though not yet being presented at a public conference by the author. Subsequently, the following yet unpublished result is presented: under the same premises, $q | h_p^-$. This generalizes a theorem of Bugeaud and Hanrot, who had proved the result under the condition $q \cdot (1 + 1/\log(p)) > p$.

Greedy sums of distinct squares

Hugh L. Montgomery

(joint work with Ulrike M. A. Vorhauer)

We represent a positive integer n as a sum of squares, using the greedy algorithm. Thus the first square s_1^2 is the largest square not exceeding n, the second square is the largest square not exceeding $n - s_1^2$, and so on. Such an expansion clearly exists and is unique. We say that n is a greedy sum of distinct squares if the summands in this expansion are unique. Let $a(n)$ be the characteristic function of this set of integers, and put $A(v) = \sum_{0 \le n < v} a(n)$. Mike Shephard asked about the natural density of this set, and conjectured that it is $1/2$. We prove that the natural density does not exist, but that the quotient $\alpha(v) = A(v)/v$ has persistent wobbles on a loglog scale, in the sense that $\alpha\big(4\exp(2^{x+k})\big)$ tends to a limit $f(x)$ as k tends to infinity through integral values. The limiting function f is continuous, non-constant, and has period 1. The values of f range between about 0.503 and 0.5096. Concerning the local behavior of the numbers $a(n)$, we note that if $s \geq 3$

then the numbers $a(s^2), a(s^2+1), \ldots, a(s^2+2s)$ are exactly the same as the numbers $a(0), a(1), \ldots, a(2s)$. In view of this highly self-replicatory nature of the $a(n)$, it is to be expected that many patterns of 0's and 1's are not found among them. Among the 2^h possible strings of 0's and 1's, let $S(h)$ denote the number of strings that actually occur as $a(n+1), a(n+2), \ldots, a(n+h)$ for some n. We find that $S(1) = 2$, $S(2) = 4$, $S(3) = 7$, $S(4) = 11$, $S(5) = 11$, $S(6) = 18$, S(7) $= 30, S(8) = 49$, $S(9) = 79$, and that for larger h the value of $S(h)$ is given by the linear recurrence

$$S(h+1) = S(h) + S(h-2) + S(h-3) + S(h-8).$$

Thus $S(h) \sim c\alpha_1^h$ as $h \to \infty$ where $\alpha_1 = 1.628668$ is the positive real root of the irreducible polynomial $x^9 - x^8 - x^6 - x^5 - 1$ and $c = 1.592655$.

Value sets of polynomials over finite fields

Gary L. Mullen

(joint work with Pinaki Das)

One of the major problems in the theory of finite fields is to be able to predict the size of the value set of a polynomial over a finite field. This problem has been studied for many years. Polynomials with maximal value sets are called *permutation polynomials* and have numerous applications in various areas. We will discuss joint work with Pinaki Das in which we improve some lower bounds on the cardinality of the value set of a polynomial over a finite field.

On the rank of appearance of the Lucas sequences

Siguna Müller

For $P, Q \in \mathbb{F}_2$, $Q \neq 0$, the Lucas sequences $U_k(P,Q)$, $V_k(P,Q)$ of first and second kind, respectively, are purely periodic over any finite field $\mathbb{F}_q$. A special type of periodicity is known as the rank of appearance (apparition). The first part of the talk deals with the number of parameters P, respectively Q, with same rank of appearance. For any possible value of the rank the corresponding result is established. The formulae for the particular type of periodicity under consideration are shown to be analogous to the number of parameters with same multiplicative order.

The explicit structure of the formulae yields a very simple mechanism for counting the number of the zeros P, respectively Q, of both of the Lucas sequences (respectively the Dickson polynomials) over $\mathbb{F}_q$.

As an application of the number of these zeros, examples of very efficient probable prime tests are given.

Solving low-degree polynomial equations: Lattice attacks on RSA

Phong Nguyen

We present Coppersmith's theorem for finding in polynomial time small roots of a monic polynomial modulo some large number of unknown factorization. We discuss applications (in cryptography and elsewhere), and extensions to multivariate polynomials (in $\mathbb{Z}/N\mathbb{Z}$ and in $\mathbb{Z}$).

Data structures for parallel exponentiation in finite fields

Michael Nöcker

Exponentiation in finite fields is a basic operation in cryptography. The basic algorithm for exponentiation is repeated squaring. We adapt this algorithm to the situation of a finite field $\mathbb{F}_{q^n}$, taking the Frobenius automorphism and different cost for multiplication (c_A) and raising to a q-th power (c_Q) in $\mathbb{F}_{q^n}$ into account.

We present a parallel algorithm for exponentiation in finite fields. This algorithm connects algorithms of Borodin & Munro (for $q = 2$ and $c_A = c_Q = 1$) and von zur Gathen (for $q \geq 2$ and $c_Q = 0$). If the algorithm works on input $c_A \geq c_Q \geq 1$ then any power of an element in $\mathbb{F}_{q^n}$ can be computed in depth at most

$$c_A \cdot \left(\lceil \log_2(q-1) \rceil + \left\lceil \log_2 \min \left\{ n, \left\lceil \frac{c_A}{c_Q} \right\rceil \right\} \right\rceil + 2 \right) + c_Q \cdot n.$$

This can be performed using $q - 1 + \min\{n, \lceil \frac{c_A}{c_Q} \rceil\}$ processors. We report on experiments using different polynomial and normal bases to represent $\mathbb{F}_{2^n}$.

A note on divisor class groups of degree zero of algebraic function fields over finite fields

Ferruh Ozbudak

We give some upper bounds on the number of degree one places of an algebraic function field over finite fields with respect to the exponent of a natural subgroup of its divisor class group of degree zero.

Pairs of coprime m-smooth polynomials over finite fields and the Waterloo algorithm for the discrete logarithm problem

Daniel Panario
(joint work with Michael Drmota)

Let $N_q(m; n)$ be the number of monic polynomials over $\mathbb{F}_q$ of degree n that are m-smooth, and let $N_q(m; n_1, n_2)$ be the number of pairs of coprime monic polynomials over $\mathbb{F}_q$ of degree n_1 and n_2 that are m-smooth. We prove that uniformly for $m, n_1, n_2 \to \infty$ with $n_1^\delta \leq m \leq n_1^{1-\delta}$, $n_2^\delta \leq m \leq n_2^{1-\delta}$ and $\delta > 0$, we have

$$N_q(m; n_1, n_2) \sim \left(1 - \frac{1}{q}\right) N_q(m; n_1) N_q(m; n_2).$$

This is proven using generating functions for the numbers $N_q(m; n)$ and $N_q(m; n_1, n_2)$, plus an application of the saddle point method for the asymptotic estimate. The range of m can be extended but the above range is enough to provide a rigorous proof for the heuristic arguments in the Waterloo variant (introduced by Blake, Fuji-Hara, Mullin and Vanstone) of the index calculus method for the computation of the discrete logarithm problem in finite fields of the form $\mathbb{F}_{2^n}$. Our proofs can be applied to any finite field $\mathbb{F}_q$.

Galois properties connected to the enumeration of permutation polynomials

Francesco Pappalardi & Claudia Malvenuto

Let $\sigma \in S(\mathbb{F}_q)$ be a permutation of the elements of a finite field $\mathbb{F}_q$ and denote by $f_\sigma(x) = \sum_{c \in \mathbb{F}_q} (1 - (x-c)^{q-1}) \in \mathbb{F}_q[x]$ its permutation polynomial. For $\sigma \neq \mathrm{Id}$, it is easy to check that the degree ∂f_σ of f_σ has the property

$$q - 2 \geq \partial f_\sigma \geq q - c(\sigma)$$

where $c(\sigma)$ is the number of elements of $\mathbb{F}_q$ moved by σ. Therefore $\partial f_\sigma = q - c(\sigma)$ is the minimum possible value for the degree. This leads one to consider the function

$$m_k(q) = \#\{\sigma \in S(\mathbb{F}_q), \sigma \text{ is a } k\text{-cycle and } \partial f_\sigma = q - k\}.$$

In a joint paper in preparation we show that

$$\frac{\varphi(k)}{k} q(q-1) \leq m_k(q) \leq \frac{(k-1)!}{k} q(q-1)$$

where the first inequality holds if $q \equiv 1(k)$ and the second holds if $q = p^k$ with $p > 2{\cdot}3^{[k/3]-1}$.

We reported on these results and announced some new ones describing the Galois structure of some algebraic sets that arise from the enumeration.

Reconstruction of geometric functions and applications

Lancelot Pecquet

More than thirty articles related to list-decoding and reconstruction have been released in the last four years, after the pioneering work of Sudan. Most of them were focused on Reed-Solomon and some algebraic-geometric codes, but the methods discussed in these papers have found some unexpected applications like, for instance, the new cryptanalysis given by Jakobsen in Crypto'98.

I will introduce a new problem of effective algebraic-geometry, that subsumes those arising in the above situations and propose an efficient algorithm to solve it. This new formulation is fairly general and provides a list-decoding and a soft-decoding algorithm for all algebraic-geometric codes.

Reduction mod p of the continued fraction of certain algebraic power series

Alf van der Poorten

Consider the continued fraction expansion of formal Laurent series over the field $\mathbb{Q}$ in the variable X^{-1}. It is easy to see by elementary heuristic considerations that generically all the partial quotients (other perhaps than some very early ones) will be linear and that their coefficients will increase in complexity at exponential rate; that is, in logarithmic height at a linear rate. Of course, it is quite another matter to prove such a thing for any particular example. By the way, over $\mathbb{F}_p$ the same heuristics say that a partial quotient has degree greater than one with probability $1/p$, greater than two, with probability $1/p^2$, and so on.

Now consider hyperelliptic curves $\mathcal{C} : Y^2 = D(X)$ with D a polynomial of degree $2g+2$ and with leading coefficient a square. Then the formal power series $\delta(X) = \sqrt{D(X)}$ will have reduction $\bmod p$ everywhere except perhaps at $p = 2$. It will have good reduction (preserving hyperellipticity) at all primes not dividing the discriminant of D. Of course modulo p, thus over $\mathbb{F}_p$, $\sqrt{D(X)}$ will always be periodic.

The sequence of complete quotients of δ (the partial quotients are the polynomial parts of those complete quotients) are all of the shape $(\delta + P)/Q$ for polynomials P of degree

$g+1$ whose leading $g+1$ coefficients coincide with those of $\delta(X)$, and polynomials Q of degree less than g. Moreover, $\deg Q = 0$ is equivalent to a period having been completed. In the elliptic case, $g = 1$, that is $\deg D = 4$, it follows that either all partial quotients (all this after the zero-th) are of degree one, or δ has a periodic expansion.

The reduction theory of continued fraction expansions of formal power series shows that partial quotients having bad reduction 'collapse' to higher degree. It follows that when $\deg D = 4$ every prime must occur in the denominator of infinitely many partial quotients and each prime p occurs periodically with period that of the period of δ expanded over $\mathbb{F}_p$. Moreover, one notes that if the n-th partial quotient has logarithmic height $O(n)$ then the n-th convergent has logarithmic height $O(n^2)$. In fact the height of those convergents is the height of the 'points' nP, where P is the divisor at infinity on the Jacobian of the curve $\mathcal{C}$.

These observations were illustrated by the examples $y^2 = x^4 - 2x^3 + 3x^2 + 2x + 1$, where δ happens to have a periodic expansion, of quasi-period 3, and $y^2 = x^4 - 2x^3 + 3x^2 + 2x + 2$, where the expansion is generic. Thus, in the former case the divisor at infinity must be a torsion divisor, in fact of order $4 = 3 + 1$. One confirms the generic nature of the second example by considering the degree of the regulator over $\mathbb{F}_p$, several p of good reduction, noting that by the reduction theory of abelian varieties its failure to be essentially invariant suffices to prove non-periodicity.

Exponential sums and lattices

Igor Shparlinski

(joint work with Isabel Gonzáles Vasco, Phong Nguyen and Edwin El Mahassni)

We describe—combining two rather different techniques—how one can create a very powerful tool for obtaining *rigorous proofs* of several results of cryptographic relevance. We show that this combination is a both-edged sword which can be used to prove *bit security* of several exponentiation based cryptographic schemes (such as Diffie-Hellman key exchange scheme, ElGamal cryptosystem, Shamir message passing scheme, XTR cryptosystem) as well as to design *provable attacks* on DSA and DSA-like signature schemes.

One of the underlying ideas goes back to D. Boneh and R. Venkatesan who introduced and studied the so-called "hidden number problem". However in many applications the "ideal distribution" settings of their approach are too restrictive. It has also turned out that the exponential sum technique (to be more precise, the uniformity of distribution results derived from bounds of exponential sums) provides a bridge which leads to a variety of new results.

Coding theory, uniform distributions, and related topics

M. M. Skriganov

We consider point sets most uniformly distributed in the unit cube. Such distributions have a rich combinatorial structure, namely, they can be completely characterized as maximum distance separable (briefly MDS) codes with respect to a non-Hamming metric in vector spaces over finite fields. This new metric had been recently introduced to coding theory by Rosenbloom and Tsfasman. It turns out that many remarkable point distributions, in particularly the distributions with a minimal order of the mean square discrepancy, can be explicitly given as codes with large weights simultaneously in the Hamming and non-Hamming metrics. This result had been recently given by William Chen

(Maquarie University, Sydney) and the author. In the course of related topics we consider MacWilliams-type theorems for the indicated non-Hamming metric. It had been recently shown by Steven Dougherty (University of Scranton, USA) and the author that a direct extension of MacWilliams identities to such a non-Hamming metric does not take place in general. Nevertheless, a more complicated generalization of MacWilliams-type theorems can be given for weight enumerators associated with orbits of a group preserving the indicated non-Hamming metric.

Lacunary polynomials

Tamás Szőnyi

In 1970 László Rédei published a book "Lückenhafte Polynome über endlichen Körpern". He developed a method for degree-estimates for lacunary polynomials, which later turned out to be very useful in finite geometry. The central problem is to estimate the number of directions determined by a set of q points in $AG(2,q)$. We survey the results on this problem from Rédei's book until the recent characterization of sets determining less than $\frac{q+3}{2}$ directions (Blokhuis, Ball, Brouwer, Storme, Szőnyi), and the result of A. Gács for $q = p$ prime, showing that a set of p points either determines $\frac{p+3}{2}$ directions (in which case it is essentially unique as Lovász and Schrijver proved), or it determines at least $\frac{2p}{3}$ directions. The results can also be applied in group theory (proofs of Burnside's theorem by Dress-Klim-Muzychuk, U. Ott; proof of Wielandt's visibility by Blokhuis-Seidel).

Computations in hyperelliptic function fields

Edlyn Teske

A hyperelliptic function field K over a finite field $k = \mathbb{F}_q$ ($q = p^t$, $p > 2$ prime) can always be represented as a real quadratic function field, i.e. $K = k(X)(\sqrt{D(X)})$ where $D(X)$ is a squarefree polynomial in $k[X]$ of degree $2g+2$ whose leading coefficient is a square in k; then g is the genus of K.

We discuss the cycle R of reduced principal ideals of a real quadratic function field K, and we show how we can make use of the arithmetic in its "infrastructure" to speed up the computation of invariants of K (such as the regulator R_X, the ideal class number h_X and the divisor class number h) in fields of small genera. If $2g+2 < \log q$, the fastest way to compute the regulator is first to compute a good approximation E of the divisor class number h and an integer L such that $|h-E| < L^2$, and then to use a square-root algorithm such as the baby-step/giant-step method or the Pollard kangaroo method to search the interval $]E-L^2, E+L^2[$ for a multiple of R_X. (Notice that $h = h_X \cdot R_X$, and in most cases R_X has a unique multiple in $]E-L^2, E+L^2[$, which is h.) With both square-root methods, we can achieve a speed-up of about $\sqrt{g}$ by cleverly exploiting the fact that we have two different operations in R, one of which is by a factor of approximately $4g$ faster than the other.

Beyond the Carlitz-Uchiyama bound

Jose Felipe Voloch

We give bounds for the number of points on $y^2 - y = f(x)$ in finite fields of characteristic two, where $f(x)$ is a polynomial. These bounds are good in a range where the Carlitz-Uchiyama bound is trivial.

On a problem of H. Cohn for character sums

Zhiyong Zheng

(joint work with T. Cochrane and D. Garth)

In this talk we introduced a problem of H. Cohn on character sums over a finite field, which asks whether a multiplicative character on a finite field can be characterized by a kind of two level autocorrelation property. The main result of this talk is the following theorem.

Theorem: (Cochrane, Garth and Zheng, 2000) *Let f be a complex valued function on the finite field F with $f(0) = 0$, $f(1) = 1$ and $|f(a)| = 1$ for all $a \neq 0$. Then f is a nontrivial multiplicative character on F if and only if for all $a, b \in F^{\times}$. We have the following "three level autocorrelation property" that*

$$(*) \qquad (q-1)\sum f(b\alpha)f(\alpha + a) = -\sum f(b\alpha)f(\alpha).$$

To answer Cohns problem, we need to show that the formula $(*)$ with $b = 1$ would implies that f is a nontrivial character of F. But a very recent work by S. Choi and K.M. Shiu indicates that Cohns conjecture is not true for an extension field, so that the only unknown case for this problem would be when F is a prime field.

A new family of exceptional polynomials

Michael Zieve

(joint work with Bob Guralnick, Peter Müller, and Joel Rosenberg)

Theorem: *Let k be an algebraically closed field of characteristic $p > 0$. There is a positive constant ε such that: for each of infinitely many integers g, there are infinitely many genus-g curves over k having at least $\varepsilon \cdot g^{3/2}$ automorphisms over k.*

The proof consists of presenting two explicit families of curves over k. These curves arise as the Galois closure of certain covers $\mathbb{A}^1_{\mathbb{F}_q} \xrightarrow{f} \mathbb{A}^1_{\mathbb{F}_q}$, where $f(x) \in \mathbb{F}_q[x]$ is an *exceptional* polynomial: i.e., the map $\alpha \to f(\alpha)$ induces a bijection on $\mathbb{F}_{q^n}$ for infinitely many n. In particular, they come from two new families of exceptional polynomials, which were described in my talk.

Edited by Michael Nöcker

Participants

Prof. Dr. Stephane Ballet
ballet@iml.univ-mrs.fr
Centre de Recherche
des Ecoles de St. Cyr
Coetquidan
F-56381 Guer Cedex

Prof. Dr. Tom Berry
berry@ldc.usb.ve
BAMCO CCS 144-00
PO Box 025322
Miami , FL 33102-5322
USA

Dr. Jürgen Bierbrauer
juergen.bierbrauer@sbg.ac.at
Institut für Reine Matheamtik
Universität Heidelberg
Im Neuenheimer Feld 288
69120 Heidelberg

Prof. Dr. Aart Blokhuis
aartb@win.tue.nl
Department of Mathematics
Technische Universiteit Eindhoven
Postbus 513
NL-5600 MB Eindhoven

Prof. Dr. Hans Dobbertin
hdobbertin@uni-klu.ac.at,
hans.dobbertin@uni-klu.ac.at
Institut für Mathematik
Universität Klagenfurt
Universitätsstr. 65-67
A-9022 Klagenfurt

Prof. Dr. Michael Fried
mfried@math.uci.edu
Dept. of Mathematics
University of California at Irvine
Irvine , CA 92697-3875
USA

Prof. Dr. John B. Friedlander
frdlndr@math.toronto.edu
Dept. of Mathematics
Scarborough College
University of Toronto
Scarborough, Ontario M1C 1A4
CANADA

Prof. Dr. Shuhong Gao
sgao@ces.clemson.edu
Dept. of Mathematical Sciences
Clemson University
Martin Hall
Clemson , SC 29634-0975
USA

Prof. Dr. Arnaldo Garcia
garcia@impa.br
Institute of Pure and Applied Math.
IMPA
Estrada Dona Castorina 110
Rio de Janeiro RJ 22460-320
BRAZIL

Prof. Dr. James W.P. Hirschfeld
jwph@sussex.ac.uk
School of Mathematical and
Physical Sciences
University of Sussex
GB-Brighton BN1 9QH

Prof. Dr. Everett Howe
however@alumni.caltech.edu
Center for Communication Research
4320 Westerra Court
San Diego , CA 92121
USA

Prof. Dr. Erich Kaltofen
kaltofen@pams.ncsu.edu
Mathematics Department
North Carolina State University
Box 8205
Raleigh , NC 27695-8205
USA

Prof. Dr. Marek Karpinski
marek@cs.uni-bonn.de
Institut für Informatik
Universität Bonn
Römerstraße 164
53117 Bonn

Prof. Dr. Sergey Konyagin
kon@mech.math.msu.su
Department of Mechanics and
Mathematics
Moscow State University
Lenin Hills
Moscow , 119899
RUSSIA

Dr. Tanja Lange
lange@exp-math.uni-essen.de
Grünstr. 11
38102 Braunschweig

Dr. Alan Lauder
lauder@maths.ox.ac.uk
Wolfson College
Oxford University
GB-Oxford OX2 6UD

Prof. Dr. Hendrik W. Lenstra, Jr.
hwl@math.berkeley.edu
Department of Mathematics
University of California
at Berkeley
Berkeley , CA 94720-3840
USA

Prof. Dr. Winnie Li
wli@math.psu.edu
Department of Mathematics
Pennsylvania State University
218 McAllister Building
University Park , PA 16802
USA

Prof. Dr. Hiren Maharaj
maharaj@math.psu.edu
maharaj@oeaw.ac.at
Inst. of Discrete Mathematics
Austrian Academy of Sciences
Sonnenfelsgasse 19
A-1010 Wien

Prof. Dr. Claudia Malvenuto
claudia@dsi.uniroma1.it
Dipartimento di Scienze
dell' Informazione
Universita di Roma "La Sapienza"
Via Salaria 113
I-00198 Roma

Dr. Helmut Meyn
meyn@immd1.informatik.uni-erlangen.de
Institut für Mathematische
Maschinen und Datenverarbeitung I
Universität Erlangen
Martensstr. 3
91058 Erlangen

Dr. Preda Mihailescu
preda@uni-paderborn.de
FB 17: Mathematik/Informatik
Universität Paderborn
33095 Paderborn

Prof. Dr. Hugh L. Montgomery
Hugh.Montgomery@math.lsa.umich.edu,
hlm@math.lsa.umich.edu
Dept. of Matheamtics
The University of Michigan
4066 East Hall
Ann Arbor MI 48109-1109
USA

Prof. Dr. Gary L. Mullen
mullen@math.psu.edu
Department of Mathematics
Pennsylvania State University
218 McAllister Building
University Park , PA 16802
USA

Peter F. Müller
peter.mueller@iwr.uni-heidelberg.de
Interdisziplinäres Zentrum
für Wissenschaftliches Rechnen
Universität Heidelberg
Im Neuenheimer Feld 368
69120 Heidelberg

Prof. Dr. Siguna Müller
siguna.mueller@uni-klu.ac.at
Institut für Mathematik
Universität Klagenfurt
Universitätsstr. 65-67
A-9022 Klagenfurt

Dr. Phong Nguyen
phong.nguyen@ens.fr
Centre de Mathematiques U.A.
Ecole Normale Superieure
45, rue d' Ulm
F-75230 Paris Cedex 05

Michael Nöcker
noecker@upb.de
FB 17: Mathematik/Informatik
Universität Paderborn
Warburger Str. 100
33098 Paderborn

Prof. Dr. Ferruh Ozbudak
ozbudak@arf.math.metu.edu.tr
Dept. of Mathematics
Middle East Technical University
06531 Ankara
TURKEY

Prof. Dr. Daniel Panario
daniel@math.carleton.edu
Dept. of Mathematics and Statistics
Carleton University
1125 Colonel By Drive
Ottawa , Ont. K1S 5B6
CANADA

Prof. Dr. Francesco Pappalardi
pappa@mat.uniroma3.it
Dipartimento di Matematica
Universita degli Studi Roma III
Largo S. L. Murialdo, 1
I-00146 Roma

Prof. Dr. Lancelot Pecquet
lancelot.pecquet@inria.fr
INRIA-Rocquencourt
Projet CODES
B.P.105
F-78153 Le Chesnay Cedex

Prof. Dr. Alfred J. van der Poorten
alf@math.mq.edu.au
Math. Department
Macquarie University
NSW 2109
AUSTRALIA

Peter Roelse
roelse@win.tue.nl
Technische Universiteit Eindhoven
Den Dolech 2
Postbus 513
NL-5600 MB Eindhoven

Dr. Hans-Georg Rück
rueck@mathematik.uni-kassel.de
FB 17 - Mathematik/Informatik -
Universität Kassel
Heinrich-Plett-Str. 40
34132 Kassel

Prof. Dr. Igor E. Shparlinski
igor@comp.mq.edu.au
School of MPCE ETA
Macquarie University
Sydney 2109
AUSTRALIA

Dr. Maxim Skriganov
skrig@pdmi.ras.ru,
asguest1@numerik.uni-kiel.de
St. Petersburg Branch of Steklov
Mathematical Institute - POMI
Russian Academy of Science
Fontanka 27
191011 St. Petersburg
RUSSIA

Prof. Dr. Henning Stichtenoth
stichtenoth@uni-essen.de
FB 6 - Mathematik und Informatik
Universität-GH Essen
45117 Essen

Prof. Dr. Tamas Szönyi
szonyi@cs.elte.hu
Department of Computer Science
Eötvös University
ELTE TTK
Muzeum krt. 6 - 8
H-1088 Budapest VIII

Dr. Edlyn Teske
eteske@cacr.math.uwaterloo.ca
Department of Combinatorics and
Optimization
University of Waterloo
Waterloo , Ont. N2L 3G1
CANADA

Prof. Dr. Jose Felipe Voloch
voloch@math.utexas.edu
Dept. of Mathematics
University of Texas at Austin
RLM 8.100
Austin , TX 78712-1082
USA

Prof. Dr. Zhiyong Zheng
zzheng@math.tsinghua.edu.cn
Department of Mathematics
Tsinghua University
Beijing 100084
CHINA

Dr. Michael Zieve
zieve@idaccr.org
Center for Communications Research
29 Thanet Rd.
Princeton , NJ 08550
USA