MATHEMATISCHES FORSCHUNGSINSTITUT
OBERWOLFACH

T a g u n g s b e r i c h t 03/1997

Finite Fields: Theory and Computation

19.01. - 25.01.1997

The first Oberwolfach Conference on Finite Fields was organized by Joachim von zur Gathen (Paderborn) and Igor Shparlinsky (Sydney). There were 31 participants from ten countries.

The talks at the meeting discussed the following areas concerning finite fields: irreducible polynomials and normal bases, value sets of polynomials, exponential sums, curves with many rational points, elliptic and hyperelliptic curves, factorization of polynomials: theory and implementations, counting problems, cryptographic applications: discrete logarithm and efficient exponentiation.

Program

Monday, 20 January 1997

9.10		Welcome
Chair: A. van der Poorten		
9.30	J. Friedlander	Distribution of inverses modulo a prime
10.20	S. Cohen	Estimates in fairly tame extensions
11.10	G. Turnwald	On the number of values of polynomials over finite fields
11.40	J. Gerhard	Polynomial factorization over finite fields
Chair: G. Mullen		
16.00	H. Niederreiter	Narrow ray class extensions and global function fields with many rational places
16.50	H. Stichtenoth	Curves over finite fields with many rational points
17.40	K. Lauter	Ray class field constructions of curves with many points

Tuesday, 21 January 1997

Chair: H. W. LENSTRA, JR.

9.10	D.-Q. WAN	Zeta functions modulo p and factoring polynomials
10.00	M. ZIEVE	Value sets and zeta functions
10.50	S. EVDOKIMOV	Factorization of polynomials over finite fields and the graph isomorphism problem
11.40	P. FLEISCHMANN	Squarefree polynomials over finite fields and regular genus numbers of classical groups

Wednesday, 22 January 1997

Chair: H. NIEDERREITER

9.10	J. VON ZUR GATHEN	Efficient exponentiation in finite fields
10.00	S. GAO	Gauß periods
10.30	P. ROELSE	Factoring high-degree polynomials over $\mathbb{F}_2$ with Niederreiter's algorithm on the IBM SP2
11.00	S. WOLF	Diffie-Hellman and discrete logarithms
11.35	I. SHPARLINSKI	Polynomial approximation of the discrete logarithm and related functions

Thursday, 23 January 1997

Chair: J. FRIEDLANDER

9.10	G. MULLEN	Irreducible polynomials over finite fields with prescribed coefficients
9.50	D. HACHENBERGER	Normal bases and completely free elements
10.45	M. KARPINSKI	Approximation algorithms for some hard counting problems in finite fields
11.35	D. GRIGORIEV	Estimating the number of zeroes of polynomial systems over finite fields

Chair: S. COHEN

16.00	W. LI	Character sums over p-adic fields
16.40	F. PAPPALARDI	Density estimates connected to Gauß periods
17.00		Problem session

Friday, 24 January 1997

Chair: G. MULLEN

9.10	F. PAPPALARDI	Average Frobenius distribution of elliptic curves
9.50	S. VLADUTS	Cyclicity statistics for elliptic curves over a finite field
10.40	G. FREY	Construction of hyperelliptic curves over finite fields
11.30	H. W. LENSTRA, JR.	Generators for the Jacobian of a hyperelliptic curve
12.15	O. MORENO	Codes, exponential sums, and Ramanujan graphs

Abstracts

STEPHEN D. COHEN: **Estimates in fairly tame extensions**

Let $f = f_1/f_2 \in k(x)$, where $k = \mathbb{F}_q$, $q = p^m$, and let $F_u = f_1 - uf_2$. f is "tame" if p does not divide the multiplicities of F_β for any $\beta \in \overline{k} \cup \{\infty\}$ and "fairly tame" if p^2 does not divide these multiplicities. The distribution of polynomials F_α ($\alpha \in k$) with a particular factorization pattern depends on the Galois group of F_u over $k(u)$ and $\overline{k}(u)$ and bounds for the genus of the splitting field. Relevant information can be derived from the ramification data and so from the multiplicities of the zeroes of F_β, $\beta \in \overline{k} \cup \{\infty\}$. We illustrate the use of "fairly tameness" in a situation which, of necessity, is non-tame.

SERGEI EVDOKIMOV: **Factoring polynomials over finite fields and the Graph Isomorphism Problem**

We show that under the Generalized Riemann Hypothesis the problem of factoring polynomials over a finite field is polynomial-time reducible to a version of the Orbit Problem for antisymmetric coherent configurations.

The Orbit Problem: given a coherent configuration on a finite set V, find the orbits of its automorphism group.

It is assumed that the set V can be given unexplicitly (for instance, as the set of the roots of a polynomial) and the oracle can be applied to a family of antisymmetric coherent configurations.

PETER FLEISCHMANN: **Squarefree Polynomials over Finite Fields and Regular Genus Numbers of Classical Groups**

Let $\mathbf{G}$ be a (simply) connected reductive linear algebraic group over $\mathbb{F}_q$ and $G = G(q) = \mathbf{G}^F$ be the corresponding finite Group of Lie type, viewed as fixed point group of a Frobenius endomorphism F of $\mathbf{G}$.
Two semisimple conjugacy classes s_1^G, s_2^G are of the same **genus** if their centralizers $C_G(s_i)$ are G - conjugate. If moreover these centralizers are abelian, the classes (or their genera) are called **regular**. In the course of computing 'generic character tables' for $G(q)$, one is interested in 'genus numbers' i.e. the numbers of semisimple classes of given genus. Of particular interest are the numbers of regular classes, which are in bijection to 'irreducible Deligne - Lusztig Characters' of the dual group G^*.

In general genus numbers can be determined by analyzing the lattices of 'stable closed subsystems' of the root system Φ of G. In the case of certain classical groups (e.g. $GL_n(q), SL_n(q), SU_n(q), Sp_{2n}(q)$) genera can also be investigated by considering characteristic polynomials of elements. The interplay between these viewpoints yields interesting connections between combinatorics of root systems and of certain types of polynomials over $\mathbb{F}_q$. In particular, by considering special squarefree polynomials one obtains, among others, explicit formulae for the

total number of regular semisimple classes in $SL_n(q), SU_n(q)$, $Sp_{2n}(q)$ and the corresponding simple groups.

GERHARD FREY: **Construction of hyperelliptic curves over finite fields**

The construction of crypto systems based on discrete logarithms in abelian groups motivates the search for hyperelliptic curves over finite fields k for which the group of k-rational points on the Jacobian J_C of C contains a subgroup of large prime order. To make this search possible one has to determine the characteristic polynomial of the Frobenius automorphism on J_C and hence to know an important part of $E = End(J_C)$. This suggests to choose E as order in a totally real field or a CM-type field and to compute the period matrix Ω of a corresponding abelian variety A. In the lecture it was sketched how one can check whether A is the Jacobian of an hyperelliptic curve $\tilde{C}$ and then to compute the equation of $\tilde{C}$ explicitely if $\dim(A) \leq 5$. By reduction one gets curves C with the desired properties.

JOHN FRIEDLANDER: **On the distribution of inverses modulo p (and other topics)**

We discussed recent joint work with Henryk Iwaniec. We gave a simple elementary proof based on ideas of A. Karatsuba of a version of Karatsuba's recent proof that one can detect cancellation in certain incomplete exponential sums of Kloosterman type where the sums run over remarkably short intervals. Because of the number of computational algorithms which rely on conjectured but unproven bounds for the least quadratic non-residue and because of the sub-exponential size of the intervals involved in this (superficially at least) similar question, we suggested the possibility that these results might find some application of that nature. We also announced our recent proof, also joint with H. Iwaniec, of the infinitude of the number of primes that can be expressed as the sum of a square and a fourth power and the asymptotic formula for the frequency of these primes.

SHUHONG GAO: **Gauss Periods**

In this talk, I presented some new theorems on Gauss periods. One is characterizing finite fields with Gauss periods that generate normal bases. Another is deciding, for any integers q, n, k and r with $nk = \varphi(r)$ and r squarefree, whether there exists a subgroup $K \trianglelefteq \mathbb{Z}_r^\times$ of order k such that $\langle q, K\rangle = \mathbb{Z}_r^\times$. In settling the latter question, an interesting theorem for finite Abelian groups is proved. The theorem goes as follows.

Suppose G is a finite Abelian group, S a subset, and K a subgroup such that $G = \langle S, K\rangle$. Then, for any direct product $G = G_1 \otimes G_2 \otimes \cdots \otimes G_t$, there exists a subgroup $H = H_1 \otimes H_2 \otimes \cdots \otimes H_t$, $H_i \trianglelefteq G_i$, such that

$$\langle S, H\rangle = G \text{ and } G/H \cong G/K.$$

JOACHIM VON ZUR GATHEN: **Efficient exponentiation in finite fields**

Computing large powers is a basic subroutine in several cryptosystems. I present several algorithms for this problem, analyze their cost, and present experimental results which confirm the theoretical analysis. In these implementations, an algorithm using Gauß periods and fast arithmetic turned out to be the winner. To increase the range of applicability of this method, we introduce a new way of forming Gauß periods.

JÜRGEN GERHARD: **Polynomial factorization over finite fields**

This is joint work with Joachim von zur Gathen. The previous five years have brought dramatic developments in the area of polynomial factorization over finite fields. For polynomials of degree n with coefficients in $\mathbb{F}_q$, the field with q elements, Kaltofen & Shoup (1995) devised the first probabilistic algorithm with subquadratic running time in the degree, taking $O(n^{1.815} \log q)$ arithmetic operations in $\mathbb{F}_q$ on average. To the progress in theory also corresponds a progress in practice: Shoup (1995) could factor a polynomial of degree 2048 modulo a 2048-bit prime in about one day of CPU-time.

Using similar techniques, in particular fast polynomial arithmetic, a blocking strategy to minimize costly gcd calculations in the distinct degree factorization stage, and an irreducibility test, leads to an algorithm for factoring polynomials over the binary field $\mathbb{F}_2$, which is no asymptotic improvement but behaves well in practice. It uses $O^{\sim}(n^2)$ arithmetic operations in $\mathbb{F}_2$, and its implementation in C++ on two Sparc Ultras with 143 MHz can factor polynomials of degree up to 262,144 in about 48 hours of CPU-time.

DIMA GRIGORIEV: **Estimating the number of non-zeroes of systems of polynomials over finite fields**

A method is developped for estimating the number of non-zeroes of systems of polynomials which was applied in two cases: for the polynomials of restricted degree and the restricted number of non-zero terms. These results entail the known lower bounds on the number of zeroes. Also the problem of zero-test is studied, i.e. to test, whether a polynomial given by a black-box, vanishes identically. The developped approach is used for solving the zero-test problem for the polynomials of the considered two classes.

DIRK HACHENBERGER: **Normal Bases and Completely Free Elements**

The central topic of my talk is the structure of the additive group of an algebraic closure Γ_F of a finite field $F = \mathrm{GF}(q)$ when considered as an F-vector space with respect to the Frobenius automorphism σ_F. It holds that the finite (F, σ_F)-submodules of Γ_F (these are the finite σ_F-invariant F-subspaces of Γ_F) are cyclic. A particular instance of the latter result is the Normal Basis Theorem for finite fields which is due to K. Hensel (1888): The finite submodules which are annihilated by polynomials of the kind $x^m - 1$ are just the finite extensions

$\mathrm{GF}(q^m)$ over F; (a generator of $E = \mathrm{GF}(q^m)$ as (F, σ_F)-module is called a *free element of E over F*; its conjugates under the Galois group of E over F build a normal basis of E over F).

Due to their usefulness for doing arithmetic computations in finite extensions over F, the algorithmic and explicit determination of (particular) normal bases has become one of the major research topics in Finite Field Theory. In my talk I will mainly concentrate on a particular type of normal bases whose existence has only been settled nearly one hundred years after Hensel's pioneering work: In 1986, D. Blessenohl and K. Johnsen proved that for every finite extension E over F there exists an element $w \in E$ which *simultaneously* generates a normal basis over *every* intermediate field K of E over F (such an element is called *completely free in E over F*).

In order to describe the nature of elements of the latter kind, we have developped tools allowing the study of Γ_F from a *simultaneous point of view*; i.e., one has to consider a finite (F, σ_F)-submodule of Γ_F with respect to *all* extensions of F leaving this module invariant. We survey on recent results concerning the characterization, the enumeration, the algorithmic, and the explicit construction of completely free elements over finite fields.

For details, I like to refer to my monograph

> FINITE FIELDS: Normal Bases and Completely Free Elements,
> Kluwer Academic Publishers (1997), Boston Dordrecht London
> ISBN: 0-7923-9851-3.
> `http://kapis.www.wkap.nl/kapis/CGI-BIN/WORLD`
> `/book.htm?0-7923-9851-3`

MAREK KARPINSKI: **Approximation Algorithms for Some Hard Counting Problems in Finite Fields**

We overview some recent results on the efficient approximability of the problem of counting the number of zeros of multivariate polynomials over finite fields. We prove also results on the approximation hardness of this problem for some classes of polynomials with lower bounds almost meeting our upper approximation bounds.

KRISTIN LAUTER: **Ray class field constructions of curves over finite fields with many rational points**

In the early 1980s, Serre applied class field theory for function fields over finite fields to obtain many examples of curves over $\mathbb{F}_2$ which are maximal for their genus. Since then, many people, including Hansen, Stichtenoth, and van der Geer and van der Vlugt, and Niederreiter and Xing have used various other methods to generate curves with a large number of points. Despite these constructions, the value of $N_q(g)$ has remained undetermined in most cases of g and q, where $N_q(g)$ stands for the maximum number of points possible on a curve of genus g over the field $\mathbb{F}_q$. The original method of Serre, as described by Rene Schoof, can

be implemented in a systematic manner for any field, and can be used to realize almost all known examples of curves with many points. By giving the ray class field description of the Deligne-Lusztig curves, we obtain the following results on the order of quotients of polynomial rings:

Theorem 1 *Let $\mathbb{F}_{q^2}$ be the finite field with q^2 elements, q a power of a prime. Let $k = q + 2$. Then*

$$|(\mathbb{F}_{q^2}[T]/T^k)^*/\mathbb{F}_{q^2}^*/\langle 1 - \alpha T \mid \alpha \in \mathbb{F}_{q^2}^*\rangle| = q$$

Furthermore, this quotient is trivial if $k < q + 2$, in which case all polynomials split completely into factors of degree one.

Theorem 2 *Let $\mathbb{F}_q$ be the finite field with $q = 2^{2m+1} = 2q_0^2$ elements. Let $k = 2q_0 + 2$. Then*

$$|(\mathbb{F}_q[T]/T^k)^*/\mathbb{F}_q^*/\langle 1 - \alpha T \mid \alpha \in \mathbb{F}_q^*\rangle| = q$$

Furthermore, this quotient is trivial if $k < 2q_0 + 2$, in which case all polynomials split completely into factors of degree one.

HENDRIK W. LENSTRA, JR.: **Generators for the Jacobian of a hyperelliptic curve**

Let k be a finite field, $q = \#k$, g a positive integer, $a, b \in k[X]$, $\deg a \leq g$, b monic of degree $2g + 1$, such that $\gcd(a^2 - 4b, (b')^2 - aa'b' + (a')^2 b) = 1$. Let C be the hyperelliptic curve of genus g defined by $y^2 + a(x)y + b(x) = 0$, and J its Jacobian. Embed C in J by $P \longmapsto [P] - [\infty]$. Finally, let I be an "interval" in k, i.e. a subset of the form $\{m, m+1, \ldots, m+n\} \cdot x + B$, where $m, n \in \mathbb{Z}$, $n \geq 0$, $x \in k$, $B \subseteq k$ an additive subgroup.

Theorem. *Suppose that $\#I \geq 4 \cdot (2g + 1) \cdot \sqrt{q}$. Then $\{(x, y) \in C(k) : x \in I\}$ generates the group $J(k)$ unless and only unless $p = \mathrm{char}\, k$ equals 2 and $I \subseteq b_{2g} + a_g^2 \cdot \ker(\mathrm{trace}: k \longrightarrow \mathbb{F}_2)$; here $b = X^{2g+1} + b_{2g}X^{2g} + \cdots$, $a = a_g X^g + \cdots$.*

In the lecture, I alluded to algorithmic applications of this theorem, due to Igor Shparlinski. Also, I indicated the proof, and how it leads me to discover the exceptional case; the latter case was illustrated in the case of elliptic curves ($g = 1$). Finally, I explained which property of "intervals" is crucial for the proof, and how the theorem can be modified to cover general I.

WINNIE LI: **Character Sums over p-adic fields**

Let K be a finite unramified extension of $\mathbb{Q}_p$. In this talk we give estimates for character sums of Weil type, such as $\sum \psi(f(x))$, $\sum \chi(g(x))$, $\sum \psi(f(x))\chi(g(x))$, where f, g are rational functions over K with integral coefficients, ψ is an additive character of K, χ is a multiplicative character of K, and the sum is over solutions of $x^{p^n} = xz^{p^n - 1}$ over K. Our method is to construct idèle class characters of the function field $k(x)$, where k is the residue field of K, and derive estimates using

the Riemann Hypothesis for curves proved by Hasse and Weil. As a consequence, we obtain a parametrization of idèle class characters of $k(x)$ using ψ and f, which allows us to construct large families of cyclically different periodic sequences with low correlation.

OSCAR MORENO: **Ramanujan graphs, codes and exponential sums**

(Joint work with H. Janwa) We introduce the notion of projective graphs of linear codes and determine that their eigenvalues are the Weil type exponential sums defined on the code. As application of our results we give several constructions of sequences of Ramanujan graphs. The proof of the Ramanujan property is given using elementary techniques.

GARY MULLEN: **Irreducible Polynomials over Finite Fields with Prescribed Coefficients**

For q a prime power let $\mathbb{F}_q$ denote the finite field of order q. We will discuss recent work involving the distribution of irreducible polynomials over $\mathbb{F}_q$ with prescribed coefficients. In particular we will discuss some recent work toward proving the existence of a primitive normal polynomial of degree $n \geq 2$ over $\mathbb{F}_q$ with an arbitrarily specified trace coefficient. A complete proof of such a result would yield a generalization of the primitive normal basis theorem for finite fields first proved by Lenstra and Schoof in 1987.

HARALD NIEDERREITER: **Narrow ray class extensions and global function fields with many rational places**

This is joint work with C. P. Xing. We present various methods for the construction of global function fields with many rational places, or equivalently of algebraic curves over $\mathbb{F}_q$ with many $\mathbb{F}_q$-rational points. We pursue two aims:

(i) get more information on the maximum number $N_q(g)$ of rational places of a global function field over $\mathbb{F}_q$ of genus g;

(ii) find explicit constructions of global function fields with many rational places.

An important role is played by Drinfeld modules of rank 1 and the narrow ray class extensions derived from them. Methods based on such extensions yield many improvements on earlier results.

FRANCESCO PAPPALARDI: **Density estimates connected to Gauß periods**

(Joint work with Joachim von zur Gathen) Let $q = p^h$ and suppose that r is a prime number with $r \equiv 1 (\mathrm{mod}\, n)$. A Gauß period of $\mathbb{F}_{q^n}$ is normal over $\mathbb{F}_q$ if and only $(i_r(q), n) = 1$ where $i_r(q) = [(\mathbb{Z}/r\mathbb{Z})^* : \langle q \rangle]$. It was proven by Wasserman that such a prime r exists if and only if $(h, n) = 1$ and

$$\begin{cases} 2p \nmid n & \text{if } p \equiv 1 (\mathrm{mod} 4) \\ 4l \nmid n & \text{otherwise.} \end{cases}$$

We prove the following variation of this result.

Suppose q and k are given and assume the Generalized Riemann Hypothesis. There always exists a prime $r \equiv 1(\mathrm{mod}k)$ such that $(i_r(q), (r-1)/k) = 1$ except when

i) h is even and k is odd;

ii) h is odd, k is odd, $p|k$ and $p \equiv 1(\mathrm{mod}4)$.

In the case $k = 1$ this result says that there exists a prime for which q is a primitive root if and only if q is not a square which is a consequence of the Artin Conjecture for primitive roots.

Furthermore we compute the density $\delta_{q,k}$ of the primes r above which is given by the formula:

$$\delta_{q,k} = \begin{cases} A_h^k & \text{if } h \text{ is even or} \\ & \text{if } h \text{ is odd, } p \not\equiv 1(\mathrm{mod}4),\ k \text{ is odd} \\ A_h^k(1 - \frac{\mu(b)}{2(2,k)-1}\prod_{l|b \atop l\nmid h}\frac{1}{l-2}\prod_{l|b \atop l|h}\frac{1}{l^2-l-1}) & \text{if } h \text{ is odd and } k \text{ is even or} \\ & \text{if } h \text{ is odd and } p \equiv 1(\mathrm{mod}4). \end{cases}$$

where $b = p/(k,p)$ and $A_h^k = \frac{1}{k}\prod_{l|k \atop l\nmid h}\left(1+\frac{1}{l}\right)\prod_{l|h \atop l\nmid k}\left(1-\frac{1}{l-1}\right)\prod_{l|h,k}\left(1-\frac{1}{l(l-1)}\right)$. The proof is a generalization of the Hooley Theorem on the Artin Conjecture.

FRANCESCO PAPPALARDI: **Average Frobenius Distribution of Elliptic Curves**

(Joint work with Chantal David, Concordia University) Let E be an elliptic curve over $\mathbb{Q}$. Let $a_p(E) = p + 1 - \#E(\mathbb{F}_p)$. If $r \in \mathbb{Z}$ then we let

$$\pi_E^r(x) = \#\{p \le x, p \text{ prime of good reduction and } a_p(E) = r\}.$$

The Lang-Trotter Conjecture states that

$$\pi_E^r \sim C_{r,E}\frac{\sqrt{x}}{\log x}$$

(except when $r = 0$ and E has complex multiplication), where

$$C_{r,E} = \frac{2}{\pi}\lim_{m\to+\infty}\frac{m \cdot \#\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})_{\mathrm{Trace}\ r}}{\#\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})},$$

where $\mathbb{Q}(E[m])$ is the extension of $\mathbb{Q}$ obtained by adding the coordinates of the m-torsion points of $E(\overline{\mathbb{Q}})$; we think of $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ as a subgroup of $\mathrm{Aut}(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z})$. Thanks to Serre's Open Mapping Theorem we know that there exists $m = m_E \in \mathbf{N}$ such that

$$C_{r,E} = \frac{2}{\pi}\frac{m_E \cdot \#\mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})_{\mathrm{Trace}\ r}}{\#\mathrm{Gal}(\mathbb{Q}(E[m_E])/\mathbb{Q})}\prod_{l\nmid m_E}\frac{l \cdot \#\mathrm{Gal}(\mathbb{Q}(E[l])/\mathbb{Q})_{\mathrm{Trace}\ r}}{\#\mathrm{Gal}(\mathbb{Q}(E[l])/\mathbb{Q})}.$$

We prove the following average form of the Lang-Trotter Conjecture. If $A, B \gg x^{1/2+\epsilon}$ and $AB \gg x^{3/2+\epsilon}$ then

$$\frac{1}{4AB} \sum_{\substack{|a| \le A \\ |b| \le B}} \pi^r_{E(a,b)}(x) \sim C_r \frac{\sqrt{x}}{\log x},$$

where $E(a,b)\colon y^2 = x^3 + ax + b$ and

$$C_r = \frac{2}{\pi} \prod_l \frac{l \cdot \#\mathrm{GL}_2(\mathbb{F}_l)_{\mathrm{Trace}\ r}}{\#\mathrm{GL}_2(\mathbb{F}_l)}.$$

PETER ROELSE: **Factoring high-degree polynomials over $\mathbb{F}_2$ with Niederreiter's algorithm on the IBM SP2**

(The following has been done in collaboration with P. Fleischmann, R. Staszewski and M. Weller). A C implementation of Niederreiter's algorithm for factoring polynomials over $\mathbb{F}_2$ is described. The most time-consuming part of this algorithm, which consists of setting up and solving a certain system of linear equations, is performed in parallel. Once a basis for the solution space is found, all irreducible factors of the polynomial can be extracted by suitable gcd-computations. For this purpose, asymptotical fast polynomial arithmetic algorithms are implemented. These include Karatsuba & Ofman multiplication, Cantor multiplication and Newton inversion. In addition, an new efficient version of the half-gcd algorithm is presented. Serial run times for the polynomial arithmetic and parallel run times for the factorization are given. It is shown that a pseudo-randomly selected polynomial of degree 300000 can be factored in about 10 hours on 256 nodes of the IBM SP2 at the Cornell Theory Center.

IGOR SHPARLINSKI: **On Polynomial Approximation and the Parallel Complexity of the Discrete Logarithm and Breaking the Diffie–Hellman Cryptosystem**

This is joint work with Don Coppersmith. Several exponential (in terms of $\log p$) lower bounds are obtained on the degrees and orders of

- polynomials;
- algebraic functions;
- Boolean functions;
- linear recurring sequences

coinciding with values of the discrete logarithm modulo a prime p at sufficiently many points (the number of points can be as little as $p^{1/2+\epsilon}$). These functions are considered over the residue ring modulo p and over the residue ring modulo

an arbitrary divisor d of $p-1$. The case of $d=2$ is of special interest since it corresponds to the representation of the rightmost bit of the discrete logarithm and defines whether the argument is a quadratic residue. These results are used to obtain lower bounds on the parallel complexity of computing the discrete logarithm.

The method is based on bounds of character sums and numbers of solutions of some polynomial equations.

Similar results are obtained for breaking the Diffie–Hellman cryptosystem. Several other applications of the method are indicated as well.

HENNING STICHTENOTH: **Curves over finite fields with many rational points**

A (projective, non-singular, absolutely irreducible) curve X defined over a finite field K of size $\#K = q^2$ is said to be maximal, if $N(X)$ (the number of K-rational points) attains the Hasse-Weil upper bound, i.e. $N(X) = q^2+1+2g(X)\cdot q$. Here, $g(X)$ denotes the genus of X.

It is well-known that the genus of a maximal curve $X/\mathbb{F}_{q^2}$ is bounded by $g(X) \leq \frac{q(q-1)}{2}$, and that the Fermat curve of exponent $q+1$ provides an example of a maximal curve of genus $\frac{q(q-1)}{2}$. In fact, it is the only curve with these properties. More precisely: Suppose that X is a maximal curve over $\mathbb{F}_{q^2}$. Then one of the following holds:

(1) $g(X) = \frac{q(q-1)}{2}$, and X is isomorphic to the Fermat curve defined by $u^{q+1} + v^{q+1} + 1 = 0$.

(2) $g(X) = \frac{(q-1)^2}{4}$, and X is isomorphic to the curve defined by $u^{q+1} + v^{\frac{q+1}{2}} + 1 = 0$.

(3) $g(X) < \frac{(q-1)^2}{4}$.

There is a similar characterisation (by means of the genus and the number of rational points) of the Deligne-Lusztig curves associated to the Suzuki groups. (Joint work with H. G. Rück, R. Fuhrmann, A. Garcia, F. Torres)

GERHARD TURNWALD: **On the number of values of polynomials over finite fields**

Let $f(x) \in \mathbb{F}_q[x]$ have degree $n \geq 1$ and let $p = \mathrm{char}(\mathbb{F}_q)$. The number $v = \#f(\mathbb{F}_q)$ satisfies $v \geq [\frac{q-1}{n}]+1$. In the case $n < p$ it is known that $v = [\frac{q-1}{n}]+1 \geq 3$ implies $n \mid q-1$ and $f(x) = a(x+b)^n + c$ (with $a, b, c \in \mathbb{F}_q$). The first part of this result can be proved under the weaker hypothesis $(n, p) = 1$. We also present improvements of various lower bounds for v if $v > [\frac{q-1}{n}] + 1$.

Let G and $\bar{G}$ denote the arithmetic and the geometric monodromy group of $f(x)$, respectively. Birch and Swinnerton – Dyer have proved that $v = cq + \mathcal{O}_n(\sqrt{q})$ where c only depends on G and $\bar{G}$ (viewed as permutation groups of degree n). In the case $\bar{G} = S_n$ one has $c = \sum_{j=1}^{n}(-1)^{j-1}/j!$. Some criteria are given which can be used to show that $\bar{G} = S_n$. By combining these it can be proved that $\bar{G} = S_n$ is possible for every n and every q. (The second part of the talk is based on joint work with M. Zieve.)

SERGEI G. VLADUTS: **Cyclicity statistics for elliptic curves over a finite field**

We calculate the probability of E (elliptic curve) over $\mathbb{F}_q$ to be cyclic. It appears that the upper limit of this probability is 1. We also characterize $\mathbb{F}_q$ with elliptic curves which are always cyclic.

DAQING WAN: **Computing zeta functions mod p and factoring polynomials over finite fields**

In the first part, we discuss general approaches (either p-adic or l-adic ($l \neq p$)) to compute the zeta function of an arbitrary algebraic variety over finite fields.

In the second part, we show how the algorithms of Berlekamp and Niederreiter on factoring polynomials in one variable over finite fields are closely related to the zeta functions mod p of the zero-dimensional varieties.

We give a new formula for the zeta functions mod p and it yields an algorithm similar to the ones of Berlekamp and Niederreiter.

In the third part, we give a very simple, explicit formula for the zeta function mod p of an arbitrary hypersurface over a finite field. This yields a polynomial time algorithm for computing the zeta function mod p if p is small (q can be large) and if the number of variables is fixed.

STEFAN WOLF: **The Diffie-Hellman Cryptosystem and Discrete Logarithms**

This is joint work with Ueli Maurer. For a cyclic group G with generator g, the Diffie-Hellman (DH) Problem is to compute, given two elements g^x and g^y, the element g^{xy}. This computation is required for breaking the Diffie-Hellman key exchange protocol. The problem is investigated if in some sense this problem is equivalent to the problem of computing discrete logarithms with respect to the generator g in the underlying group G. For a certain class of groups, the two problems are shown to be probabilistic polynomial-time equivalent: this is the case if the order of the DH group G is such that all the large prime factors of the group order $|G|$ are single, and such that for each such prime factor p a suitable auxiliary group, defined in some way over the field $GF(p)$, with smooth order is given. Possible auxiliary groups are elliptic curves and Jacobians of hyperelliptic curves over $GF(p)$ and extension fields, as well as subgroups of the multiplicative group of such an extension field. In particular it is shown that when the group

order $|G|$ of G is a prime p, and $p-1$, $p+1$, or $\Phi_n(p)$ for some small n is smooth, then the DH protocol for G is as secure as the DL problem is difficult.

MICHAEL ZIEVE: **Value Sets and Zeta Functions**

Let n be a fixed positive integer. A result of Birch and Swinnerton-Dyer implies that there is a finite set of rational numbers such that, for any finite field $\mathbb{F}_q$ and any polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n, we have $\#f(\mathbb{F}_q)/q = c + O_n(1/\sqrt{q})$, where c is in our finite set of rational numbers. (Here $\#f(\mathbb{F}_q)$ denotes the cardinality of the image of the map $f\colon \mathbb{F}_q \to \mathbb{F}_q$ induced by $\alpha \mapsto f(\alpha)$.) We first reviewed the little that is known about these rational numbers c: they satisfy $c \cdot n! \in \mathbb{Z}$, $1/n \le c \le 1$, and indeed either $c = 1$ or $c = 1 - 1/n$ or $c \le 1 - 2/n$. Also, for 'general' polynomials, $c = 1 - 1/2! + 1/3! - \ldots \pm 1/n!$. Evidence suggests that there are many further restrictions on the values c, and it would be very interesting to have a fuller picture. We then discussed the problem of constructing all polynomials achieving a prescribed value of c; there is significant partial work in the case $c = 1$, and the cases $c = 1 - 1/n$ and $c = 1 - 2/n$ can be completely resolved (a new result). Interestingly, in all known examples with these three values of c, the splitting field of $f(x) - t$ over $\mathbb{F}_q(t)$ is either a rational function field or a Hermitian function field. Next we turned to the error term $O_n(1/\sqrt{q})$, which essentially comes from the Weil bound. We proposed to approach the finer structure of this error term via a 'value set zeta function', namely $\exp(\sum_{i=1}^{\infty} \#f(\mathbb{F}_{q^i})T^i/i)$. We gave a preliminary approach to the study of this object, which shows that it has several pleasant properties. Still, the theory is in its infancy; but one can hope that one day these zeta functions will shed light on the values c, as well as explain various mysterious examples in which the value set seems to be 'too well-behaved'.

Author: JÜRGEN GERHARD

List of email addresses

COHEN, STEPHEN D.	sdc@maths.gla.ac.uk
EVDOKIMOV, SERGEI A.	evdokim@pdmi.ras.ru
FLEISCHMANN, PETER	peter@exp-math.uni-essen.de
FREY, GERHARD	frey@exp-math.uni-essen.de
FRIEDLANDER, JOHN B.	frdlndr@math.toronto.edu
GAO, SHUHONG	sgao@math.clemson.edu
VON ZUR GATHEN, JOACHIM	gathen@uni-paderborn.de
GERHARD, JÜRGEN	jngerhar@uni-paderborn.de
GRIGORIEV, DIMA A.	dima@cse.psu.edu
GURAK, STANLEY	gurak@pwa.acusd.edu
HACHENBERGER, DIRK	hachenberger@math.uni-augsburg.de
JUNGNICKEL, DIETER	jungnickel@math.uni-augsburg.de
KARPINSKI, MAREK	marek@cs.uni-bonn.de
LAUTER, KRISTIN	lauter@mpim-bonn.mpg.de
LENSTRA, JR., HENDRIK W.	hwl@math.berkeley.edu
LI, WINNIE	wli@math.psu.edu
MORENO, OSCAR	o_moreno@upr1.upr.clu.edu
MULLEN, GARY	mullen@math.psu.edu
MYERSON, GERRY	gerry@mpce.mq.edu.au
NIEDERREITER, HARALD	niederreiter@oeaw.ac.at
PAPPALARDI, FRANCESCO	pappa@mat.uniroma3.it
VAN DER POORTEN, ALFRED J.	alf@mpce.mq.edu.au
ROELSE, PETER	roelse@exp-math.uni-essen.de
SCHIFFELS, GERHARD	schiffel@mathematik.uni-bielefeld.de
SHPARLINSKI, IGOR E.	igor@mpce.mq.edu.au
STICHTENOTH, HENNING	stichtenoth@uni-essen.de
TURNWALD, GERHARD	turnwald@uni-tuebingen.de
VLADUTS, SERGEI	vladut@lmd.univ-mrs.fr (until June 1997) vladut@ippi.ac.msk.ru (from July 1997)
WAN, DAQING	wan@math.psu.edu
WOLF, STEFAN	wolf@inf.ethz.ch
ZIEVE, MICHAEL	zieve@math.brown.edu

Tagungsteilnehmer

Dr. Stephen D. Cohen
Department of Mathematics
University of Glasgow
University Gardens

GB-Glasgow , G12 8QW

Prof.Dr. Shuhong Gao
Dept. of Mathematical Sciences
Clemson University
Martin Hall

Clemson , SC 29634-1907
USA

Prof.Dr. Sergei A. Evdokimov
St. Petersburg Institute for
Informatics and Automation
14th Liniya 39

199178 St. Petersburg
RUSSIA

Prof.Dr. Joachim von zur Gathen
FB 17: Mathematik/Informatik
Universität Paderborn
Warburger Str. 100

33098 Paderborn

Dr. Peter Fleischmann
Institut für Experimentelle
Mathematik
Universität-Gesamthochschule Essen
Ellernstr. 29

45326 Essen

Jürgen Gerhard
FB 17: Mathematik/Informatik
Universität Paderborn
Warburger Str. 100

33098 Paderborn

Prof.Dr. Gerhard Frey
Institut für Experimentelle
Mathematik
Universität-Gesamthochschule Essen
Ellernstr. 29

45326 Essen

Prof.Dr. Dima A. Grigoriev
Dept. of Computer Science & Eng.
Pennsylvania State University
State College

University Park , PA 16802
USA

Prof.Dr. John B. Friedlander
Dept. of Mathematics
Scarborough College
University of Toronto

Scarborough, Ontario M1C 1A4
CANADA

Prof.Dr. Stanley Gurak
Dept. of Math. and Comp. Sciences
University of San Diego

San Diego , CA 92110-2492
USA

Dr. Dirk Hachenberger
Institut für Mathematik
Universität Augsburg

86135 Augsburg

Prof.Dr. Winnie Li
Department of Mathematics
Pennsylvania State University
218 McAllister Building

University Park , PA 16802
USA

Prof.Dr. Dieter Jungnickel
Institut für Mathematik
Universität Augsburg

86135 Augsburg

Prof.Dr. Oscar Moreno
Dept. of Mathematics
Faculty of Natural Sciences
University of Puerto Rico
Box 23355

Rio Piedras , PR 00931
USA

Prof.Dr. Marek Karpinski
Institut für Informatik
Universität Bonn
Römerstraße 164

53117 Bonn

Prof.Dr. Gary L. Mullen
Department of Mathematics
Pennsylvania State University
218 McAllister Building

University Park , PA 16802
USA

Prof.Dr. Kristin Lauter
Max-Planck-Institut für Mathematik
Gottfried-Claren-Str. 26

53225 Bonn

Dr. Gerry Myerson
c/o Mr. L. Myerson
3419 Irwin Ave @503

Bronx , NY 10463
USA

Prof.Dr. Hendrik W. Lenstra, Jr.
Department of Mathematics
University of California
at Berkeley
721 Evans Hall

Berkeley , CA 94720-3840
USA

Prof.Dr. Harald Niederreiter
Inst. für Informationsverarbeitung
Österreichische Akademie
der Wissenschaften
Sonnenfelsgasse 19

A-1010 Wien

Prof.Dr. Francesco Pappalardi
Dipartimento di Matematica
Universita degli Studi Roma III
Via C. Segre, 2

I-00146 Roma

Prof.Dr. Henning Stichtenoth
FB 6 - Mathematik und Informatik
Universität-GH Essen

45117 Essen

Prof.Dr. Alfred J. van der Poorten
School of MPCE
Macquarie University

Sydney NSW 2109
AUSTRALIA

Dr. Gerhard Turnwald
Mathematisches Institut
Universität Tübingen
Auf der Morgenstelle 10

72076 Tübingen

Peter Roelse
Institut für Experimentelle
Mathematik
Universität-Gesamthochschule Essen
Ellernstr. 29

45326 Essen

Prof.Dr. Sergei G. Vladuts
IML
Luminy case 930

F-13288 Marseille Cedex 9

Prof.Dr. Gerhard Schiffels
Fakultät für Mathematik
Universität Bielefeld
Postfach 100131

33501 Bielefeld

Prof.Dr. Da-Qing Wan
Department of Mathematics
Pennsylvania State University
218 McAllister Building

University Park , PA 16802
USA

Prof.Dr. Igor E. Shparlinski
School of MPCE ETA
Macquarie University

NSW 2109
AUSTRALIA

Stefan Wolf
Institut für theoretische
Informatik
ETH-Zentrum

CH-8092 Zürich

Dr. Michael Zieve
Department of Mathematics
Brown University
Box 1917

Providence , RI 02912
USA

Gefördert durch
DFG Deutsche Forschungsgemeinschaft