Report

on the Second Dagstuhl Seminar on

Algorithms and Number Theory

October 10 – 14, 1994

Algorithms in number theory play an important role in computer science as well as in mathematics. The main purpose of this Dagstuhl seminar was to bring together experts in both fields to exchange ideas and discuss open problems concerning all aspects of the theory and practice of number theoretic algorithms. The topics treated comprised factoring integers and polynomials, computing discrete logarithms, constructions in finite fields, procedures in lattice theory, algorithms on number fields and computations with elliptic curves and other diophantine equations. An emphasis was laid on the computer scientific point of view.

The 47 participants of the seminar came from 12 countries. Aside from the official program of lectures there was ample opportunity for discussions of topics of joint interest concerning algorithms and number theory. The special atmosphere of Schloss Dagstuhl contributed a lot to a stimulating and productive workshop.

The organizers would like to thank all participants for their contributions to a successful seminar.

Schedule of the Dagstuhl-Seminar "Algorithms and Number Theory"

Monday, October 10, 1994

Morning session. Chairman: Claus P. Schnorr

9^{00}- 9^{10}	Johannes Buchmann:	Opening
9^{10}- 9^{55}	Henri Cohen:	Computing in Relative Extensions of Number Fields
10^{00}-10^{20}	Francisco Diaz y Diaz:	Tables of Number Fields
10^{40}-11^{10}	Victor S. Miller:	A Problem of Harvey Cohn
11^{15}-12^{00}	George Havas:	Extended GCD Algorithms: Old and New

Afternoon session. Chairman: Jacques Martinet

15^{00}-15^{45}	Claus P. Schnorr:	Pruned Enumeration in Lattice Reduction
15^{50}-16^{35}	Brigitte Vallee:	An Analysis of the Gaussian Algorithm for Lattice Reduction
16^{50}-17^{20}	Istvan Gaàl:	Application of Thue Equations to Computing Power Integral Bases in Algebraic Number Fields
17^{25}-17^{55}	Attila Pethoe:	Quadratic Polynomial Values in Second Order Linear Recurrence Sequences

Tuesday, October 11, 1994

Morning session. Chairman: Michael Pohst

9^{00}- 9^{45}	John Cremona:	Computation of Modular Elliptic Curves, a Progress Report
9^{50}-10^{20}	Josef Gebel:	On Mordell's Equation
10^{40}-11^{25}	Jean M. Couveignes:	Elliptic Curves in Small Characteristic
11^{30}-12^{00}	Volker Müller:	Finding the Eigenvalue in Elkies' Algorithm

Afternoon session. Chairman: Nikos Tzanakis

15^{00}-15^{30}	Christian Batut:	Construction of Cyclotomic Lattices
15^{35}-16^{15}	Jacques Martinet:	Eutactic Lattices
16^{30}-17^{15}	Francois Morain:	On Character Sums
17^{20}-17^{55}	Renate Scheidler:	Computation of Residuosity Symbols

Wednesday, October 12, 1994

Morning session. Chairman: Arien K. Lenstra

9^{00}- 9^{20}	Ken Nakamula:	Certain Quartic Fields with Explicite Fundamental Units
9^{25}- 9^{55}	Alf van der Poorten:	Families of Special Quadratic Number Fields
10^{00}-10^{20}	Franz Lemmermeyer:	Computation of Ideal Class Groups of Bicyclic Biquadratic Number Fields
10^{40}-11^{00}	Michael Jacobson:	Some Numerical Experiments Concerning Quadratic Fields
11^{05}-11^{35}	Roel Stroeker:	Consecutive Cubes Summing up to a Perfect Square
11^{40}-12^{00}	Johannes Buchmann:	LiDIA – A Library for Computational Number Theory

Afternoon: Excursion

Thursday, October 13, 1994

Morning session. Chairman: Henri Cohen

9^{00}- 9^{30}	Arjen K. Lenstra:	Factoring
9^{35}-10^{05}	Dan Bernstein:	The Number Field Sieve
10^{10}-10^{40}	Oliver Schirokauer:	Using Number Fields to Compute General Discrete Logarithms NFS
11^{00}-11^{30}	Victor Shoup:	Distributed Polynomial Factorization
11^{35}-12^{05}	Harald Niederreiter:	Factoring Polynomials Using Differential Equations: an Update

Afternoon session. Chairman: John Cremona

15^{00}-15^{30}	Mario Daberkow:	On Computing Bases in Relative Radical Extensions
15^{35}-15^{55}	Michael Pohst:	On Solving Relative Norm Equations
16^{00}-16^{20}	Nigel P. Smart:	Sieving an S-unit Equation
16^{35}-17^{05}	Nikos Tzanakis:	Finding Explicitly all Integral Solutions of a Quartic Elliptic Equation
17^{10}-17^{30}	Chris Smyth:	Bezout's Theorem and Euclid's Algorithm
17^{35}-18^{00}	Wolfgang Schwarz:	On Class Numbers of Abelian Number Fields

Friday, October 14, 1994

Morning session. Chairman: Alf van der Poorten

9^{00}- 9^{20}	Michel Olivier:	Galois Groups for Polynomials of Degree 11
9^{20}- 9^{55}	Herman Te Riele:	Amicable Number Tripels
10^{00}-10^{30}	Igor Shparlinski:	Approximate Constructions in Finite Fields
10^{50}-11^{20}	Valeri I. Korjik:	The Progress in Iterative Decoding Algorithms

Henri Cohen

Computing in Relative Extensions of Number Fields

We show how the usual algorithms valid over z can be extended to the ring of integers z_K of an algebraic number field. We give an extended Euclidean algorithm, a canonical Smith and Hermite normal form, algorithms to find them, and applications to the usual problems of algebraic number theory: a relative round 2 algorithm for computing integral (pseudo) bases and relative discriminants, prime ideal factorization, relative class group and unit computations, etc.

The basic idea is the following (trivial) proposition: If a, $b \in z_K$ and $\mathcal{D} = az_K + bz_K$ is the ideal generated by a and b, then we can in polynomial time find u, $v \in \mathcal{D}^{-1}$ such that $au + bv = 1$.

Fransisco Diaz y Diaz

Tables of Number Fields

This is the announcement that the Computational Group in Number Theory of Bordeaux has decided to regroup all the tables of number fields, insofar as complete tables of reasonable length are available to us.

These tables will be completed, if necessary, by adding whatever arithmetic data we are able to compute. The correctness of class group and fundamental unit data is guaranteed only under the GRH.

For the number fields that we know the following data will be available:

1 A monic polynomial generating the field; a root α of this polynomial is one of the smallest primitive elements in the ring of integers for the L_2 norm.

2 The signature of the field.

3 The Galois group of the Galois closure of the field.

4 The discriminant of the number field and the index of $K[\alpha]$ in the ring of integers.

5 An integral basis.

6 The class number. The structure of the class group as a product of cyclic groups. An ideal a in a class generating these cyclic groups. A generator of a raised to the power of the order of the corresponding cyclic group.

7 The regulator.

8 The number of roots of unity in the field and a generator of the torsion part of the unit group.

9 A system of fundamental units.

The tables under consideration are tables of degrees 3,4,5 and 6 for all possible signatures and tables of totally real fields of degree 7. All these tables will be available by anonymous ftp.
This presentation is a first step towards more extensive computations concerning these number fields.

Victor S. Miller

A Problem of Harvey Cohn

Harvey Cohn posed the problem

$$\begin{aligned} \text{If} \quad & f: \ \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{R}, \ (p \text{ odd prime}) \\ & f(0)=0, \ f(1)=1, \ |f(k)=1| \text{ for } k \neq 0, \\ & \text{and} \sum_{y=0}^{p-1} f(y)f(y+k) = -1 \text{ for } k \neq 0, \\ \text{then is} \quad & f(k) = \left(\frac{k}{p}\right). \end{aligned}$$

A proof (due to H.W. Lenstra) is given. The problem is generalized:

$$\begin{aligned} \text{If} \quad & f: \ \mathcal{F} \longrightarrow \mathbb{C}\,, \ (\mathcal{F} \text{ finite field}) \\ & f(0)=0, \ f(1)=1, \ |f(k)=1| \text{ for } k \neq 0, \\ & \text{and} \sum_{y=0}^{p-1} \overline{f(y)}f(y+k) = -1 \text{ for } k \neq 0, \\ \text{then is} \quad & f \text{ a character of } \mathcal{F}^* \end{aligned}$$

If $\mathcal{F}$ is not the prime field this must be modified to

$$\text{then is} \quad f = \chi \circ \rho, \ \text{where } \rho \text{ is an additive automorphism.}$$

When deg$\mathcal{F}$ is even this is not true by a construction of H.W. Lenstra and V. Miller. When $\mathcal{F}$ is a prime field calculations are determined for $p = 3, 5, 7$ (the latter took $\sim$ 52000 seconds) which shows the conjecture is true.

George Havas

Extended gcd Algorithms: Old and New

(Joint work with Bohdan S. Majewski; partially supported by the Australian Research Council)

We consider the complexity of expressing the greatest common divisor of n numbers as a linear combination of the numbers. Our interest in this problem arises from a study of Smith and Hermite normal form computations for integer matrices. To improve the efficiency of such computations, we concentrate our efforts on the phase where the first entry of the first row (or column) is made the greatest common divisor of the first entry of all rows (or columns). If we have n rows then this is the problem of computing the gcd of a set of n integers in a good way for our application. This means finding a good set of multipliers in an extended gcd calculation.

On the one hand we prove the NP-completeness of finding optimal sets of multipliers with respect to both the L_0 metric and L_∞ norm. On the other side we present and analyze a new method for expressing the gcd of n numbers as their linear combination and give an upper bound on the size of the largest multiplier produced by this method, which is optimal. In an appropriate model of computation the algorithm is both time and space optimal. However this algorithm is only of theoretical interest.

We also present some well-performing practical algorithms. A relatively fast algorithm is based on sorting the numbers whose gcd is being computed and performing quotient/remainder steps on close pairs of numbers. Better multipliers can be obtained using lattice basis reduction algorithms at the expense of increased execution time. We compare the performance of these algorithms with previous methods which may be exponentially worse in terms of multiplier size.

Claus P. Schnorr

Pruned Enumeration in Lattice Reduction

We propose a pruned depth first enumeration of short lattice vectors which is based on the fact that the expected number of vectors of an arbitrary lattice L in a sphere S of fixed radius and random center is vol $S/$ det L. If a random lattice basis $b_1, \ldots, b_m$ is given so that the reduced vector of Gram-Schmidt coefficients ($\{\mu_{i,j}\}$ $1 \leq j < i \leq m$) is uniformly distributed in $[0, 1)^{\binom{m\Gamma 1}{2}}$ then the pruned enumeration finds with fixed positive probability a shortest lattice vector. The combination of pruned enumeration with block reduction yields the most powerful lattice reduction algorithms to date. We demonstrate the power of these algorithms by solving random subset sum problems of arbitrary density in dimension 82.

Brigitte Vallee

Average-case analysis af the Gaussian Algorithm for lattice reduction

The Gaussian algorithm is a lattice analogue of the classical Euclidean algorithm. It is based on a lifting of the real shift operator U of continued fractions

$$U(x) = (\frac{1}{x}) - [\frac{1}{x}] \quad \text{(where } [x] \text{ denotes the integer part of real } x\text{)}$$

into a complex operator

$$U(z) = (\frac{1}{z}) - [\mathrm{Re}(\frac{1}{z})],$$

which is formed with an inversion-symmetry followed by an integral translation. When applied to a complex z that belongs to disk $\mathcal{D}$ with diameter $\mathcal{I} = [0, 1]$, the inversion brings z outside of the disk then the translation brings it inside the strip $\mathcal{B} = \{z \mid 0 \leq \mathrm{Re}(z) \leq 1\}$. The Gaussian algorithm is then a sequence of iterations of the operator U.

```
Input: $z \in \mathcal{D}$
Output: $z \in \mathcal{B} \backslash \mathcal{D}$.
While $z \in \mathcal{D}$ do $z := U(z)$.
```

The average-case analyses of the Gaussian algorithm and of the Euclidean algorithm are quite different. We study here the random variable L representing the number of iterations, when the inputs z are distributed inside $\mathcal{D}$ with an initial density f. We obtain two main results:
(1) The random variable L is asymptotically geometrically decreasing. More precisely, if $\rho(\ell)$ denotes the probability of the event $[L \geq \ell + 1]$, the ratio $\rho(\ell + 1)/\rho(\ell)$ admits a limit ρ when ℓ tends to infinity.
(2) The distribution of the inputs inside disk $\mathcal{D}$ during the execution of the algorithm admits a limit form : if $F_0 = f$ denotes the initial density of the inputs z inside $\mathcal{D}$ and F_ℓ is the density inside $\mathcal{D}$ after ℓ iterations, then there exists a limit density F_∞ of the F_ℓ.
Our proofs make use of a family of operators $\mathcal{H}_s$ that generalize the Ruelle-Mayer operators $\mathcal{G}_s$. For complex s with $\Re(s) > 1$, the two families are defined by

$$\mathcal{G}_s f(t) = \sum_{m \geq 1} (\frac{1}{(m+t)^s} f(\frac{1}{m+t}), \qquad \mathcal{H}_s f(t) = \sum_{m \geq 1} (\frac{1}{|m+t|^s} f(\frac{1}{m+t}).$$

These operators can be viewed as the inverses of the shift operator U with the $\mathcal{G}$ family being the holomorphic version of the $\mathcal{H}$ family.
The properties of the $\mathcal{G}$ family are well-known: for s real and $s > 1$, the

operator $\mathcal{G}_s$ satisfies a Perron-Frobenius theorem. It has a unique dominant eigenvalue, denoted by $\lambda(s)$ and a unique associate eigenvector g_s, under the normalization $g_s(0) = 1$. The average-case analysis of the Euclidean algorithm relies on the "dominant" eigenvalue properties of $\mathcal{G}_s$ in a neighbourhood of $s = 2$; the limit density is then proportional to dominant eigenvector g_2 defined by $g_2(t) = 1/(1+t)$, and it does not depend on the initial density inside $\mathcal{I}$.

The average-case analysis for the Gaussian algorithm uses the family $\mathcal{H}_s$. When defined on a "natural" set of functions which are simultaneously analytic with respect to real variables x and y, the operators $\mathcal{H}_s$ have the same "dominant" behaviour as their holomorphic analogues $\mathcal{G}_s$. The two limit quantities, the ratio ρ of the probability distribution and the limit density F_∞, depend on the initial density. More precisely, they depend on the valuation of the initial density near the real axis. (One says that a positive function f defined on $\mathcal{D}\backslash\mathcal{I}$ has valuation t near the real axis if there exists a continuous function g on $\mathcal{D}$, strictly positive on $\mathcal{I}$, for which one has $f(x,y) = |y|^t\; g(x,y)$.)

For an initial density with valuation t ($t > -1$), the limit objects exactly correspond to dominant spectral objects of the operator H_{4+2t}: the limit ρ of ratio $\rho(\ell+1)/\rho(\ell)$ is equal to the dominant eigenvalue $\lambda(4+2t)$ of $\mathcal{H}_{4+2t}$, while the limit density F_∞ has valuation t and is proportional to the dominant eigenvector $g_1(4+2t)$ of $\mathcal{H}_{4+2t}$.

For an initial density that is uniform, the limit ratio ρ equals $\lambda(4) \equiv 0.1993$. For an initial density f whose valuation t tends to -1, the inputs tend to concentrate in $\mathcal{I}$ and the behaviour of the Gaussian algorithm tends to be the same as the Euclidean algorithm. In that case, the limit ratio ρ tends to $\lambda(2) = 1$.

As a final conclusion, the family of operators $\mathcal{H}_s$ provides a unified framework for the the average-case analysis of both algorithms.

Istv án Gaál

Application of Thue Equations to Computing Power Integral Bases in Algebraic Number Fields

Let κ be an algebraic number field of degree n. It is an old problem in algebraic number theory to decide if κ has a power integral basis, that is an integral basis of the form $\{1, \alpha, \ldots, \alpha^{n-1}\}$. This problem is equivalent to the resolution of index form equations

$$(*) \qquad I(x1, \ldots, x_n) = \pm 1 \text{ in } x_1, \ldots, x_n \in z$$

where $I(x1, \ldots, x_n)$ is a form of degree $\frac{n(n-1)}{2}$. The resolution of these equations seems to be a hard problem, especially for higher degree number fields.

It turns out, however, that these equations can often be reduced to certain types of Thue equations.
For cubic number fields $(*)$ is itself a cubic Thue equation.
For quartic number fields $(*)$ can be reduced to a cubic Thue equation and to some corresponding quartic Thue equations.
For $n > 4$ the resolution of $(*)$ is only hopeful if κ admits some proper subfields which implies that $I(x1, \ldots, x_n)$ is reducible. For this reason as a next step we considered the resolution of $(*)$ in totally real sextic number fields. In this case $(*)$ has already 5 variables and degree 15. It turns out that for such fields $(*)$ can be reduced to a relative Thue equation of degree 3 over the quadratic subfield of κ and to some corresponding equations having the same structure as an inhomogeneous Thue equation of degree 3.

Attila Peth ö

Quadratic Polynomial Values in Second Order Linear Recurrence Sequences

We present a direct method, which results from the dipohantine equation

$$G_n = a * x^2 + b * x + c,$$

where G_n denotes the n-th term of a second order linear recurrence sequence, a linear form in logarithms of algebraic numbers. As application we prove the following two theorems:
Theorem: *Let $a \geq 4$ be an integer, $\Delta = a^2 - 4, \alpha = (a + \sqrt{\Delta})/2$ and $\beta = (a - \sqrt{\Delta})/2$. Then the diophantine equations*

$$\frac{\alpha^n - \beta^n}{\alpha - \beta} = 2, 22, 32, 62$$

have no solutions in n for $n > 3$ except when $a = 338$ and $n = 4$.

Theorem: *The system of diophantine equations*

$$x^2 - 6y^2 = -5, \qquad x = 2z^2 - 1$$

has only the following solutions

$(x, \pm y, \pm z) = (-1, 1, 0), (1, 1, 1), (7, 3, 2), (17, 7, 3), (71, 29, 6), (16561, 6761, 91).$

The results were proved jointly with M. Mignotte, Strasbourg.

John Cremona

Computation of Modular Elliptic Curves, a Progress Report

Since the tables of all modular elliptic curves of conductors up to 1000 were published in 1992, substantial progress has been made in this project, both of a quantitative and of a qualitative nature. The programs have been completely rewritten (in C++ from ALGOL68) and now incorporate numerous improvements. For example, structured Gaussian elimination techniques result in a large saving in running time when solving the modular symbol relations. To date, all (isogeny classes of) curves of conductors up to 4000 have been found (with a very few exceptions), numbering 13351 classes, and it is expected to pass 5000 by the end of this year. This should settle the question of whether 5077 is the minimal conductor of a curve of rank 3.

A partially experimental new method was also described for computing a curve attached to each newform: this method is very much faster than an exact determination of the full period lattice, but is not guaranteed to find the strong Weil curve. Also, it does not deliver other data of interest such as the degree of the modular parameterization.

Josef Gebel

On Mordell's Equation

By the theorem of Mordell, the Mordell–Weil group $E(\mathbb{Q})$ of an elliptic curve over the rational numbers $\mathbb{Q}$ is finitely generated, i.e. any point $P \in E(\mathbb{Q})$ can be represented as

$$(*) \qquad P = \sum_{i=1}^{r} n_i P_i + T \quad (n_i \in Z)$$

where $\{P_1, \ldots, P_r\}$ denotes a basis of the free part of $E(\mathbb{Q})$ and T is a torsion point. Our goal was to determine all integral points $P = (x, y),\ x, y \in Z$, on a series of elliptic curves, the Mordell curves

$$E_k : \quad y^2 = x^3 + k \qquad (k \in Z)$$

for all k in absolute value smaller than some bound K.

Together with H.G. Zimmer (Saarbrücken) and A. Pethö (Debrecen), the author developed a method that computes an upper bound N such that

$$P \text{ is integral } \Longrightarrow |n_i| \leq N \ \forall\ 1 \leq i \leq r$$

in the representation $(*)$ of P.

Using this method, we determined all integral points on E_k for $|k| <= 2500$ and listed the results like the rank, a basis, the torsion group, the regulator, the Tate–Shafarevič group, all integral points etc. in a table.

Jean-Marc Couveignes

Elliptic Curves in Small Characteristic

The computation of the cardinality of some elliptic curve E over a finite field F_q where $q = p^k$ can be achieved using Schoof's algorithm and the improvements proposed by Atkin, Elkies and Atkin again. Elkies idea involves the computation of some isogeny of degree l from E when it exists, i.e. when l is a small auxiliary *good* prime. To achieve this goal, Elkies uses recurrence formulae between modular forms which happen to become trivial as soon as the degree l of the isogeny becomes greater than the characteristic p.

We explained how to solve this problem using the formal groups associated to both the elliptic curve and its isogeneous curve.

We took this opportunity to recall a few quite basic facts about formal groups of height one in finite characteristic, such as their isomorphism classification, their endomorphism ring, the Hasse invariant and Lazard's polynomials. We briefly presented the lines of our algorithm and the experimental preliminary results obtained at the École Polytechnique by Reynald Lercier and François Morain. Those results, concerning finite fields with characteristic 2, already improve on previous ones obtained by Vanstone and alii using Schoof and Atkin's ideas.

Volker M üller

Finding the Eigenvalue in Elkies' Algorithm

(joint work with Frank Lehmann, Markus Maurer, Victor Shoup)

The algorithm of Atkin/Elkies is the best known algorithm for counting the number of points on an elliptic curve over a large finite prime field. One important part of this algorithm includes the search for an eigenvalue of the Frobenius endomorphism of an elliptic curve. I discuss several algorithms for doing this search, especially I present a new variant of a baby-step giant-step algorithm, which proved in practice quite efficient. One important step of this algorithm is a fast method for finding in a table of rational functions one special function which is equivalent modulo a polynomial to some given rational function. This method is based on ideas of Victor Shoup.

I report on the use of these ideas in our implementation of the Atkin/Elkies algorithm to count the number of points on a curve over the prime field $\mathcal{F}_p$, where p is a 425-digit prime.

Christian Batut

Computations of Cyclotomic Lattices

Following ideas of Thomson, Feit, Craig, E. Bayer, Quebbemann, we study even modular lattices of level l and study then properties of extremality in the sense of Sloane (modular forms). We describe a family $B_{n,l}^{(m)}$ of lattices constructed on the quadratic field $\mathbb{Q}(\sqrt{-l})$ and the cyclotomic field $\mathbb{Q}(\zeta_p)$. This family includes $B_{8,1}^{(1)} = E_8$, $B_{12,3}^{(1)} = K_{12}$, $B_{24,1}^{(2)} = \Lambda_{24}$ and other interesting modular lattices.

Jacques Martinet

Classification of Eutactic Lattices

(joint work with Anne-Marie Bergé)

Let E a Euclidean space of dimension n. For a lattice Λ in E, let S be its set of minimal vectors, and, for $x \in S$, let p_x be the orthogonal projection on the line $\mathbb{R}x$. We say that Λ is eutactic if there exists a linear combination $\mathrm{Id}_E = \sum_{x\in S} \rho_x p_x$ with strictly positive coefficients ρ_x, and that it is perfect if the p_x's span $\mathrm{End}^s(E)$.

Voronoi characterized in 1907 the extreme lattices (the lattices for which the density is a local maximum) as those which are both perfect and eutactic, and proved the finiteness of the set of perfect lattices (up to similarity). Avner Ash proved in 1977 that the same result holds for eutactic lattices.

Our contribution to the subject is:

1. We introduce the notion of weak eutaxy, for which we drop the sign condition on the ρ_x's. Thus, whereas convexity is involved in eutaxy, weak eutaxy is a linear notion.

2. We define a partition of the set of all lattices in finitely many "minimal classes".

3. We prove that each class contains at most ONE weakly eutactic lattice.

4. We prove that the weakly eutactic lattice of a given class (if any) is the less dense in this class.

5. We prove that any weakly eutactic lattice can be scaled to an algebraic one.

6. We classify eutactic lattices up to dimension 4.

In a paper of 1980, Avner Ash gave a "mass formula with signs" for the eutactic lattices in a given dimension. Here is the formula for dimensions 2, 3, 4. (The denominators are the orders of the group of automorphisms of determinant +1.)

$$-\frac{1}{4} + \frac{1}{6} = -\frac{1}{12} \,(= \zeta(-1))\,.$$

$$-\frac{1}{24} + \frac{1}{24} + \frac{1}{12} - \frac{1}{8} + \frac{1}{24} = 0\ ;$$

$$\frac{1}{192}-\frac{1}{120}-\frac{1}{48}-\frac{1}{48}+\frac{1}{12}+\frac{1}{16}+\frac{1}{144}-\frac{1}{8}-\frac{1}{8}-\frac{1}{48}+\frac{1}{8}+\frac{1}{8}-\frac{1}{72}-\frac{1}{12}+\frac{1}{120}+\frac{1}{576} = 0\,.$$

François Morain

On Character Sums

(Joint work with A. Joux, to appear in *J. Number Theory.*)

Let d be an odd prime $\equiv 3 \bmod 4$ such that the quadratic field $K = \mathbb{Q}(\sqrt{-d})$ has class number 1. Let $E_d : y^2 = x^3 + a_d x + b_d$ with rational integer coefficients have complex multiplication by the ring of integers of K. We note ω_1 and ω_2 the periods of E_d. Let p be a prime. We are interested in the computation of

$$S_d(p) = \sum_{x=0}^{p-1} \left(\frac{x^3 + a_d x + b_d}{p} \right)$$

(where (a/p) denotes the Legendre symbol). By complex multiplication, we know that if $(-d/p) = -1$, then $S_d(p) = 0$ and that if $(-d/p) = +1$, then $4p = u^2 + dv^2$ with u and v rational integers and $S_d(p) = \pm u$.

The correct determination of the sign is difficult. It is known for $d \in \{7, 11, 19\}$. For computing this sign, we use Rajwade's method that we simplify and express in a suitable way using the notion of $\sqrt{-d}$-division points. If $\wp$ is the Weierstrass function of E_d, these values are $x_r = \wp(r\omega_2/\sqrt{-d})$ for $1 \leq r \leq (d-1)/2$. We show that the x_r's are integers in $\mathbb{Q}(\cos(2\pi/d))$ and we compute the decomposition of x_r as

$$x_r = \sum_{k=0}^{(d-1)/2} a_{r,k} \cos(2\pi r/d)$$

with the a_r's rational integers using LLL. The corresponding ordinates y_r (such that $y_r^2 = x_r^3 + a_d x_r + b_d$) are shown to be in $\mathbb{Q}(\sqrt{2}, \cos(2\pi/d))$ and their exact value determined in the same way with LLL. Using this, we can compute the correct sign of $S_d(p)$ for all values of d in $\{43, 67, 163\}$.

We show that our method can be used when the class number of K is greater than 1, in some cases, including $d = 15$. For $d = 5$, we refer to some other work of the author and F. Leprévost.

Renate Scheidler

Computation of Residuacity Symbols

Residuacity symbols are an extension of Jacobi symbols to cyclotomic fields of odd prime order. A higher order law of reciprocity plus complementaries, analogous to the quadratic law of reciprocity and its complementaries for -1 and 2, were first given by Kummer. These can be used to compute residuacity symbols quickly. As in the quadratic case, this technique relies heavily on Euclidean division. A very fast Euclidean division method based on ideas of Lenstra can be used to evaluate residuacity symbols of order up to 11.

Due to McKenzie, it is known that the fields of order 13, 17, and 19 are norm-Euclidean, but here the division algorithms are slower and much more cumbersome. In fact, no fast such technique is currently known for these cases. Furthermore, cyclotomic fields of prime order at least 23 do not even have unique prime factorization. The question of how to possibly replace Euclidean division in order to compute residuacity symbols in these fields rapidly remains open.

Ken Nakamula

Certain Quartic Fields with explicit Fundamental Units

For

$$(s,\, t,\, u) \in \mathbb{N} \times \mathbb{Z} \times \{\pm 1\} \quad \text{with} \quad (s,\, t,\, u) \neq (1,\, -1,\, 1),$$

define a polynomial $f \in \mathbb{Z}[X]$ by

$$f = X^4 - sX^3 + (t+2u)X^2 - usX + 1.$$

Put

$$D_1 := s^2 - 4t, \quad D_2 := (t+4u)^2 - 4us^2$$

and let

$$K = \mathbb{Q}(\varepsilon), \quad K_2 = \mathbb{Q}\left(\sqrt{D_1}\right), \quad L_2 = \mathbb{Q}\left(\sqrt{D_1 D_2}\right).$$

Here ε is a zero of f.
We assume that

$$D_1 \text{ and } D_2 \text{ are both discriminants of quadratic fields.}$$

Then K is a non-CM quartic field with a quadratic subfield K_2, non-Galois over $\mathbb{Q}$, and the composite KL_2 is dihedral over $\mathbb{Q}$ cyclic over L_2. Moreover the unit rank $r(K)$ of K is given by

$$r(K) = \begin{cases} 1 & \text{if } D_1 < 0, \\ 2 & \text{if } D_2 < 0, \\ 3 & \text{otherwise.} \end{cases}$$

For each rank $r(K) = 1,\, 2,\, 3$, we construct infinitely many K which satisfy the assumption and have explicit fundamental units in terms of ε.

Alf van der Poorten

Families of special Quadratic Number Fields

It remains an interesting problem to detect infinite families of positive integers D for which one can readily describe the fundamental unit of the quadratic number field $\mathbb{Q}(\sqrt{D}\,)$. I (and Hugh Williams - this is joint work) deal with a class of cases $D = F(X)$, where F is a polynomial of even degree and with leading coefficient a square, for which one obtains particularly small units, because the period length is essentially independent of the integer parameter X. That of course means a particularly large class number for the fields $\mathbb{Q}(\sqrt{D}\,)$. We rediscover all quadratic polynomials F with the said property and provide recipes permitting one to detail the period of the continued fraction for the various cases.
The context is a theorem of Schinzel who shows that if F is an integer valued polynomial, either of odd degree, or of even degree with its leading coefficient not a square, then as the integer X varies one has $\overline{\lim}\,\ell(\sqrt{F(X)}\,) = \infty$; here $\ell(\delta)$ denotes the length of the period of the continued fraction expansion of the quadratic irrational δ. On the other hand, in the quadratic case Schinzel shows that $\overline{\lim}\,\ell(\sqrt{F(X)}\,) < \infty$ if and only if $F(X) = A^2X^2 + BX + C$ with discriminant $\Delta = B^2 - 4A^2C \neq 0$ and $\Delta \,|\, 4 \cdot \gcd(2A^2, B)^2$. Well known examples of such F include the Richaud-Degert types: $A^2X^2 \pm A$, $A^2X^2 \pm 2A$, and $A^2X^2 \pm 4A$, which provide periods of length at most 12. Subsequently, Stender had determined the fundamental unit of $\mathbb{Q}(\sqrt{D}\,)$ when $D = F(X)$ with F quadratic as above, provided that $\gcd(A^2, B, C) = 1$.
We show that in the quadratic case Schinzel's condition, together with gcd (A^2, B, C) squarefree, in effect entails that the approximation $|AX| + B/2A$ to $\sqrt{F(X)}$ provides the first half of a period of $\sqrt{F(X)}$. Thus, aside from some possibly degenerate cases with $|X|$ small, the period of $\sqrt{F(X)}$ is not just of bounded, but is in fact of constant length. This is not quite so. If $F(X) \equiv 1 \bmod 4$ and both numerator and denominator of the approximation $|AX| + B/2A$ are odd then the expansion of that approximation provides just the first sixth of the period. The other sixths are its 'twists' in a sense readily explained. Plainly, in this case the length of the period depends on the parity of X. More generally, if $G^2 \div \gcd(A^2, B, C)$ then again the period is some multiple of that evident first part, with the other parts twisted by multiplication by G; again the length depends on the parity of $|X| \bmod G$.

Franz Lemmermeyer

Computation of Ideal Class Groups of Bicyclic Biquadratic Number Fields

It is well known that the identity

$$2 = 1 + \sigma + 1 + \tau + 1 + \sigma\tau - (1 + \sigma + \tau + \sigma\tau)$$

in the group ring $Z[G]$ (where $G =< \sigma, \tau >$ is Klein's 4-group) can be used to compute the unit group of an extensions K/F, where $Gal(K/F) = G$, from the unit groups of its subfields. If the class number of F is odd, class field theory gives a formula for the index $(Cl(K) : C)$, where C is the subgroup of ideal classes in K which are generated by ideals from the subfields. If there are only a few ramified primes in K/F, this index is small, and the identity above may be used to compute the structure of the ideal class group $Cl(K)$ from the class groups of the subfields of K/F (for details, see http://www.math.uiuc.edu).

Michael J. Jacobson, Jr.

Some Numerical Experiments Concerning Quadratic Fields

(Joint work with R.F. Lukes and H.C. Williams)
It is well known that the non-torsion part of the unit group of a real quadratic field κ is cyclic. With no loss of generality we may assume that it has a generator $\varepsilon_o > 1$, called the fundamental unit of κ. The natural logarithm of ε_o is called the regulator R of κ. In this paper the following problems are considered:

1. How big (small) can R get?
2. How often does this occur?

The answers to these questions are simple when considering the problem of how small R can be, but seem to be extremely difficult when we are dealing with the problem of how large R can get. In order to investigate this, several large-scale numerical experiments, involving the Extended Riemann Hypothesis and the Cohen-Lenstra class number heuristics, were conducted. These experiments provide numerical confirmation to what is currently believed about the magnitude R.

Roel Stroeker

Consecutive Cubes Summing up to a Perfect Square

In this talk, I considered the problem of determining all integral solutions to the Diophantine equation

$$\sum_{i=1}^{n}(x+i-1)^3 = y^2, \tag{1}$$

for $n = 2, 3, \ldots$, apart from the trivial ones given by $x = 0$ and $x = 1$. J.W.S. Cassels [*A Diophantine Equation*, Glasgow Math. J. **27** (1985), 11–18] considered the case $n = 3$. The method he uses is rather ad hoc and hence not suitable for generalization. A more general approach is to make use of the structure of the elliptic curve $E_n(\mathbb{Q})$ given by (1). This elliptic curve may be put into short Weierstraß form

$$Y^2 = X^3 + \frac{1}{4}n^2(n^2 - 1)X, \tag{2}$$

by means of the transformation

$$(x, y) \longmapsto (X, Y) = \left(nx + \tfrac{1}{2}n(n-1), ny\right).$$

These elliptic curves have the following properties:

- $E_n(Q)$ has torsion group $\mathbf{Z}/2\mathbf{Z}$,
- $r_n := \operatorname{rank}(E_n(Q)) \geq 1$, and also an upper bound for the rank can be given in terms of n.

Now let P be any integral point on (2), let $P_1, \ldots, P_{r_n}$ be a Mordell-Weil basis for $E_n(Q)$, and let $P_0 = (0, 0)$ be the non-trivial torsion point. Use is made of a lower bound of linear forms in elliptic logarithms recently obtained by S. David to compute an upper bound for $\max_i |m_i|$ in

$$P = m_1 P_1 + \ldots + m_{r_n} P_{r_n} + \varepsilon P_0,$$

where $\varepsilon \in \{0, 1\}$. This upper bound is reduced by de Weger's implementation of the LLL-algorithm to manageable proportions. The method is explained in detail in [R.J. Stroeker and N. Tzanakis, *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arithm. **67** (1994), 177–196]. Complete sets of solutions were given for all n between 2 and 50, and for $n = 98$. Of these 50 equations, only 16 have no non-trivial solutions. In this range 21 rank 1 curves, 22 rank 2 curves and 6 rank 3 curves were found; the first rank 4 curve occurs for $n = 98$.

Johannes Buchmann

LiDIA – A Library for Computational Number Theory

In early 1994 our research group in computational number theory at the Department of Computer Science of the Universität des Saarlandes, Germany, was working on implementations of algorithms for factoring integers, determining discrete logarithms in finite fields, counting points on elliptic curves

over finite fields, etc. In those implementations three different multiprecision integer packages were used. The code written for those implementations was hard to read and hardly documented as well. Therefore, many basic routines were written over and over again, often not very efficiently.
In this situation we decided to organize the whole software in a library which we called LiDIA. We agreed on the following design principles:

- Efficiency; we try to provide the user with a very good implementation of the best algorithms available.
- Modularity; the dependency of parts of the library on each other is kept to a minimum; interfaces are clearly described so that replacing modules by more efficient modules is very simple.
- Portability; except for a small kernel which exists for different architectures and which can be easily replaced, LiDIA runs on any machine with an appropriate CPP compiler.
- Good documentation; all LiDIA programs are described by a manual page similar to the Unix manual pages; online documentation is available.
- Interactive availability; for learning and experementing, the LiDIA functions can be accessed interactively.

Although not in the public domain, LiDIA can be used freely for non commercial purposes. A first LiDIA release will be available via ftp@crypt1.cs.uni-sb.de on November 30 1994.

Arjen K. Lenstra

Factoring

Currently the two most practical general purpose algorithms for the factorization of integers are the Quadratic Sieve Method (QS) and the Number Field Sieve Method (NFS). In April 1994 a new QS- record was set with the factorization of the 129-digit number 'RSA-129', a challenge number that was published in 1977 in Martin Gardner's column in Scientific American. Back then it was believed that factoring RSA-129 would require more than 40 quadrillion years. Its QS-factorization took 8 months on a world-wide network of more than 1000 computers (using their idle time only). The total computing time spent on the factorization is approximately 5000 MIPS years.
Even though NFS is asymptotically superior to QS, it was long believed

that the crossover point between QS and NFS is beyond our current range of interest. Recent improvements in our NFS implementations have shown, however, that NFS is already faster than QS for relatively small numbers: the NFS-factorization of a 116-digit general number was completed in about half the time QS would have spent on it, and other experiments indicate that NFS can even be further improved. These recent improvements might have far-reaching consequences for the security of cryptosystems based on widely used 512-bit RSA technology.

Daniel J. Bernstein

The Number Field Sieve (sort of)

An integer $n > 1$ is a *perfect power* if it is of the form m^k, $k > 1$. How quickly can we tell if n is a perfect power? I have an algorithm which runs in time essentially

$$B(n) = \sum_{2 \le p \le \log_2 n} (\log_2 p)(\log_2 n - \log_2(1 + |n - (\operatorname{round} n^{1/p})^p|)).$$

On average, and in the normal case, $B(n)$ is essentially linear in $\log_2 n$. I hope that the same is true of the worst case. This algorithm has several variants, all of which seem just as difficult to analyze.

Oliver Schirokauer

Using Number Fields to Compute General Discrete Logarithms

Let p be a rational prime and let $q = p^n$. We present an algorithm to solve the discrete logarithm problem in $\mathcal{F}_q$. Our method is based on the algorithm of Gordon ([1]) and the author's own work on logarithms in prime fields ([3]). The algorithm we give makes use of many of the techniques of the number field sieve and has a conjectured expected running time of

$$L_q[1/3; (64/9)^{1/3} + o(1)],$$

where

$$L_q[s; c] = \exp(c(\log q)^s (\log \log q)^{1-s}),$$

and the limit implicit in the $o(1)$ is for n fixed and $p \to \infty$. This is the same time needed to factor a number the size of q using the number field sieve. Let $\prod l^e$ be the prime factorization of $q - 1$. The goal of our algorithm is to compute, for a given prime factor l, an integer x_l such that $t^{-x_l} v$ is an l^eth power. In this case, $\log_t v \equiv x_l \bmod l^e$. The Chinese Remainder Theorem can then be used to compute $\log_t v$.

To find x_l, we use an approach similar to that of the number field sieve factoring algorithm. Recall that in this algorithm one first constructs an extension $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ with special properties which I do not discuss here and then combines smooth elements in both $\mathbb{Z}(\alpha)$ and $\mathbb{Z}$ to form squares. In our case, the base field of the field extension is no longer $\mathbb{Q}$ but a number field in which p is a prime of degree n and the multiplicative combinations of smooth elements in the two fields are not squares but l^eth powers. In order to identify such powers we introduce a map λ which can be thought of as an approximation of the l-adic logarithm and which has the property that an algebraic integer δ is very likely to be an l^eth power if the order of each prime ideal dividing (δ) is a multiple of l^e and if $\lambda(\delta) = 0$. In fact, if λ is a sufficiently good approximation of the l-adic logarithm, then it is a consequence of Leopoldt's conjecture that δ is an l^eth power. In this way, Leopoldt's conjecture arises as one of the assumptions of our algorithm.

References.

[1] D.M. Gordon, Discrete logarithms in $GF(p)$ using the number field sieve, SIAM J. Discrete Math. **6** (1993), 124-138.

[2] J.P. Buhler, H.W. Lenstra, Jr., Carl Pomerance, Factoring integers with the number field sieve, The development of the number field sieve (A.K Lenstra, H.W. Lenstra, Jr., eds.), Lecture Notes in Mathematics **1554** (1993), Springer-Verlag, Berlin, 50-94.

[3] O. Schirokauer, Discrete logarithms and local units, Theory and applications of numbers without large prime factors (R.C. Vaughan, ed.), Philosophical Transactions of the Royal Society, Series A, **345** (1993), The Royal Society, London, 409-423.

Victor Shoup

Factoring Polynomials over Finite Fields

Two new algorithms are presented for factoring a polynomial over a finite field.

The first algorithm (joint work with Erich Kaltofen) runs in time $O(n^{1.815}\log q)$ on input polynomials of degree n over F_q. This result is somewhat theoretical, as it depends on fast matrix multiplication.

The second algorithm runs in time $O(n^{2.5} + n^{1+\epsilon}\log q)$, and has been proven to be quite effective in practice. Empirical data from experiments comparing this algorithm with Berlekamp's algorithm are presented which indicate that this new algorithm is significantly faster and more space efficient. In particular, when q is a large prime, we are able to factor much larger polynomials than was previously possible.

Harald Niederreiter

Factoring polynomials using differential equations: an update

New deterministic factorization algorithms for polynomials over fields of positive characteristic were presented by the speaker at the first Dagstuhl Workshop on Algorithms and Number Theory in 1992. These algorithms are based on new types of linearizations of the factorization problem using differential equations. Since 1992 a lot of work was done on these algorithms, and the talk gives a report on the current state of affairs. In the case of finite fields, the new algorithms are preferable to the deterministic Berlekamp algorithm if the characteristic is small. A survey on the new algorithms is available in the speaker's paper "New deterministic factorization algorithms for polynomials over finite fields", Contemporary Math., Vol. 168, pp. 251-268, American Math. Society, 1994.

Mario Daberkow

On computing Bases in Relative Radical Extensions

Let $\mathcal{E}/\mathcal{F}$ be a radical extension of an algebraic number field, e.g $\mathcal{E} = \mathcal{F}(\sqrt[n]{\mu})$ with $n \in \mathcal{N}$ and μ an integral element of $\mathcal{F}$. We present an algorithm for the computation of an integral basis of $\mathcal{E}$ with relative methods.

In the first step we study Kummer extensions $\mathcal{E}/\mathcal{F}$ of prime degree p. As a result we explicitly construct a system of $\wr_F$–generators of $\wr_E$, where $\wr_F$ and $\wr_E$ are the rings of integers of $\mathcal{F}$ and $\mathcal{E}$, respectively. The construction is based on a theorem of Hecke, which describes the relative discriminant discEF of such an extension $\mathcal{E}/\mathcal{F}$. This theorem can be modified for local Kummer extensions to derive the generators for associated global extensions. The result on Kummer extensions of prime degree leads to an algorithm for the computation of the ring of integers of $\mathcal{E}$ for arbitrary Kummer extensions $\mathcal{E}/\mathcal{F}$ and then for radical extensions $\mathcal{E}/\mathcal{F}$.

We finally present several examples for integral bases of radical extensions $\mathcal{E}/\mathcal{F}$ with $[\mathcal{E} : \mathcal{Q}]$ up to 1300.

Michael E. Pohst

On solving Relative Norm Equations

We report on joint work with A. Jurk and C. Fieker. Let $E \subset F$ be algebraic number fields of degree m, mn over $\mathcal{Q}$, respectively. Let o_E, o_F be the rings of integers of E, F, and let $M \subset F$ be a free unital o_E-module. For a given

$\kappa \in o_E$, we discuss the problem of solving

$$N_{E/F}(x) \ = \ \kappa \ \text{ in } \ x \in M \ \ . \qquad (3)$$

The solution presented is analogous to the absolute case. It requires bounds for the conjugates of potential solutions x. If the unit group U_F of F satisfies

$$U_F M \subseteq M$$

, such bounds can be derived for all elements of a complete system of non-associate solutions. The only prerequisite for this is an appropriate choice of fundamental units for F. Then all solutions can be computed as lattice points in a finite number of suitable ellipsoids. A rough estimate of the number of required arithmetical operations indicates that this number is exponential in n but polynomial in m. Various numerical examples support this observation. They also demonstrate the advantage of the new method over the older (absolute) one of solving the norm equation (1) by exhibiting the solutions among those of $N_{E/\mathcal{Q}}(x) \ = \ N_{F/\mathcal{Q}}(\kappa)$.

Nigel Smart

Sieving An S-Unit Equation.

In this talk the author explained one motivation for studying general two term S-unit equations. Namely the completion of lists of curves of genus two with bad reduction at two only. These have been computed by Merriman (1970), Top (1984) and Merriman and Smart (1993, 1994). However all of these approaches have problems. Sieving S-unit equations was first performed by Tzanakis and de Weger, the speaker explained his small prime version which considerably speeds up the computing time.

Nikos Tzanakis

Solving elliptic quartic diophantine equations by estimating linear forms in elliptic logarithms

We extend the method developed in [ST] and [GPZ] to the solution in integers of diophantine equations of the form $V^2 \ = \ Q(U)$, where Q is an polynomial with integer coefficients,with non-zero discriminant. As in the above mentioned papers,the method makes use of the arithmetical theory of elliptic curves, transcendental numbeer theory (a theorem of S. David on lower bounds of linear forms in elliptic logarithms) and reduction techniques based on the LLL-algorithm. However, the use of the isomorphism between the elliptic curve E associated to the given equation and the additive group

R/Z, defined in [Z],is not now as direct as in the case of the cubic elliptic equations studied in [ST] and [GPZ] and requires extra technical work. As an application we solve very easily equations of this type found in the litterature,some of which are well known for their difficult and tricky solution. It is interesting to note that in all such difficult examples,the rank of the corresponding elliptic curves is 1 or 2.

References.

[GPZ] J. Gebel, A. Pethoe, H. Zimmer, Computing integer points on elliptic curves Acta Arithm. 68 (1994),171-192.
[ST] R. Stroeker, N. Tzanakis, Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms, Acta Arithm. 67 (1994),177-196.
[Z] D. Zagier, Large integer points on elliptic curves, Math. Comp. 48 (1987),425-436.

Chris Smyth, Edinburgh University

Bezout's Theorem and Euclid's Algorithm

We describe an algorithm for computing the intersection multiplicities of two curves in $C[x, y]$. The algorithm is recursive, and based on Euclid's algorithm for polynomials in x. It seems to work more efficiently than algorithms using resultants.

One can also use the same idea to define the intersection of the two curves (as a multiset of their intersection points) from which most of the properties of the intersection follow, including Bezout's theorem.

This algorithm was developed with a view to applications on high degree highly singular models for elliptic and other curves. The idea is to use such models to specify a priori rational points on the curve. In the case of genus 1, the group law can then be given using intersections of the original curve with certain so-called adjoint curves. This is a generalisation of the "chord and tangent" process for non-singular cubic models of the curve.

Wolfgang Schwarz

On the Class Number of a Real Abelian Number Field

Let p be an odd prime and K a real abelian number field of conductor not divisible by p^2. We define K to be p-regular if for every character $\chi \neq 1$ of K $L_p(1\chi)$ is a p-adic unit. This implies that the class number $h(K)$ is not divisible by p. If the conductor of K is prime to p, p-regularity can be tested efficiently using the Fermat quotient; this goes back to Leopoldt. We give an explicit formula for the coefficients of the Fermat quotient, namely

$$Q_p(1-\zeta) = \sum_i a_i \zeta^i, \text{ with } a_i = \sum_{j=1}^{[ip/m]} j^{-1}m^{-1} \bmod p,$$

where ζ is a primitive m-th roots of unity. To test whether all conjugates of a character are p-regular, you just have to test whether the polynomial $\sum_{(i,m)=1} a_i X^{\lambda(i)}$ is coprime to the m-th cyclotomic polynomial mod p; here $\lambda(i)$ is defined by $\chi(i) = \zeta^{\lambda(i)}$. In a few special cases, it can be shown that the field is p-regular; namely, if q is a prime such that p is a primitive root mod q: if $l = 2q+1$ is prime and $l > p$, then $\mathbb{Q}(\zeta_l)^+$ is p-regular (this is due to Jakubec); if $l = 4q+1$ is prime and $l > 4p$, then the subfield of $\mathbb{Q}(\zeta_l)^+$ of degree q is p-regular, and if $l > p^2 + p$, then $\mathbb{Q}(\zeta_l)$ is p-regular iff $\mathbb{Q}(\sqrt{l})$ is p-regular.

Michel Olivier

Galois Groups for Polynomials of Degree 11

We present the continuation of a previous work concerned with the computation of the Galois groups of the polynomials in $\mathbf{Z}[X]$ (cf. Dagstuhl-Seminar-Report;39, 22.06.-26.06.92 (9226), p.7). We determine the Galois group of a polynomial using the old method of resolvents.

For degree $n = 10$ or $n = 11$, for each transitive subgroup G of degree n in S_n, consider all the transitive subgroups H of degree n of S_n having the property:

$(*)$ at least one conjugate of H by element of S_n is included in G.

For all pairs of transitive groups (H, G) where H is maximal among all the groups possessing the property $(*)$, we give an invariant polynomial and the corresponding resolvent which allow us to compute the Galois group of the polynomials of degree n.

We describe some tables of polynomials of degree 10 and 11 with a given Galois group.

Herman J.J. te Riele

Amicable Number Triples

Let $\sigma(m)$ denote the sum of all the divisors of m. Amicable number triples, introduced by L.E. Dickson, are triples of positive integers (m_1, m_2, m_3), $m_1 \leq m_2 \leq m_3$, for which:

$$\sigma(m_1) = \sigma(m_2) = \sigma(m_3) = m_1 + m_2 + m_3.$$

An example is the triple

$$(1980,\ 2016,\ 2556) = (2^2 3^2 5 \cdot 11,\ 2^5 3^2 7,\ 2^2 3^2 71).$$

L.E. Dickson (*The Amer. Math. Monthly* **20** (1913) 84-92) has found ten amicable number triples, and P. Poulet (*La Chasse aux Nombres*, Fasc. I, Parfaits, amiables et extensions, Bruxelles, 1929) published 145 of such triples. In this talk a new method is presented to find amicable number triples: a positive integer s is chosen in a suitable way, and as many as possible solutions of the equation $\sigma(x) = s$ are computed; next, it is checked whether among the found solutions there are triples which sum up to s.

Example 1: for $s = 3 \cdot 8! = 120960 = 2^7 3^3 5 \cdot 7$ we computed 123 solutions of the equation $\sigma(x) = s$ and among them there are *three* triples which sum up to s. The smallest is

$$(37380,\ 41412,\ 42168) = (2^2 3 \cdot 5 \cdot 7 \cdot 89,\ 2^2 3 \cdot 7 \cdot 17 \cdot 29,\ 2^3 3 \cdot 7 \cdot 251).$$

Example 2: for $s = 13!$ we found 27561 solutions of the equation $\sigma(x) = s$, and among them there are 689 triples which sum up to s.

The method is also suitable for finding amicable k-tuples, with $k > 3$, i.e., k-tuples $(m_1, \cdots, m_k)$ of positive integers for which

$$\sigma(m_1) = \cdots = \sigma(m_k) = m_1 + \cdots + m_k.$$

With growing k, however, it becomes increasingly time-consuming to find k-tuples which sum up to s, from a given big list of solutions of the equation $\sigma(x) = s$.

Our method is a generalization of a method to find amicable number *pairs* (H.J.J. te Riele, *A new method to find amicable pairs*, Proceedings of the Vancouver Conference "Mathematics of Computation 1943-1993", AMS Proceedings of Symposia in Applied Mathematics, 1994, to appear), but it generates many more amicable triples than amicable pairs.

Igor Shparlinski

Approximate Constructions in Finite Fields

There are two classical problems in the theory of finite fields: given a prime p and integer n, construct a finite field $\mathcal{F}_q$ of $q = p^n$ elements and given a finite field $\mathcal{F}_q$ find a primitive root of $\mathcal{F}_q$.

Unfortunately, no deterministic polynomial time algorithm is known for either of these problems. We consider their relaxed "approximate" versions which are quite enough for many applications and give an outline of known

fast (polynomial time in a number of cases) “approximate” algorithms. An incomplete list of applications includes:
FFT over finite fields, Matrix Multiplication Testing, Sparse Polynomial Interpolation, Coding Theory, Cryptography, Combinatorial Designs, Pseudo-Random Number Generation.

Valeri I. Korjik

The Progress in Iterative Decoding Algorithms

We consider the maximal likelihood estimate of key, which has been developed in the paper (Andelman, Reeds “On the Cryptanalysis of Rotor Machines and Substitution-Permutation Networks”, IEEE on Inf. Th., 4, 1982.) The feature of this approach is to embed the deterministic key space in a continued one. At first the likelihood function as a function of key probabilities for a stream cipher produced by LFSR and nonlinear combiner is presented. Then we introduce a modified Andelman-Reeds iterative algorithm to compute extreme values of this function. We can not prove a convergent of this algorithm in general case and then we use simulation.
For LFSR with length 31 and the nonlinear combiner as Jeffe generator we obtain correct results after 140 iterations. In the general case the complexity of this cryptanalysis is about $O(N \cdot s \cdot n^2)$, where N is the length of the cryptogram, s is the number of the output of LFSR, n is the length of the LFSR.

Christian **Batut**
Université Bordeaux I
UFR de Mathémathiques et
Informatique
351 Cours de la Libération
F-33405, Talennce Cedex
France
batut@ceremab.u-bordeaux.fr
tel.:+33-56-84-60-96

Dan **Bernstein**
University of California at Berkeley
Department of Mathematics
Berkeley, CA 94720
USA
djb@silverton.berkeley.edu
tel.:+1-510-643-5933

Johannes **Buchmann**
Universität des Saarlandes
Fachbereich 14 - Infornatik
Postfach 151150
D-66041 Saarbrücken
Germany
buchmann@cs.uni-sb.de
tel.:+49-681-302 4156

Henri **Cohen**
Université Bordeaux I
UFR de Mathémathiques et
Informatique
351 Cours de la Libération
F-33405, Talennce, Cedex
France
cohen@ceremab.u-bordeaux.fr

Jean-Marc **Couveignes**
ENS – Paris
Ecole Normale Superieure
Département de Mathémathiques
45 Rue d'Ulm
F-75230 Paris, Cedex 05
France

John **Cremona**
University of Exeter
Department of Mathematics
North Park RD,
Exeter, EX4 4QE
Great Brirtain
cremona@maths.exeter.ac.uk
tel.:+44-392-263974

Mario **Daberkow**
TU Berlin
Fachbereich 3 Mathematik
sek. Ma 8-1
Straße des 17. Juni 136
D-10623 Berlin
daberkow@math.tu-berlin.de
tel.:+49-30-314 251 69

Thomas **Denny**
Universität des Saarlandes
Fachbereich 14 - Infornatik
Postfach 151150
D-66041 Saarbrücken
Germany
denny@cs.uni-sb.de
tel.:+49-681-302 4168

Francisco **Diaz y Diaz**
Université Bordeaux I
UFR de Mathémathiques et
Informatique
351 Cours de la Libération
F-33405, Talennce, Cedex
France
diaz@ceremab.u-bordeaux.fr
tel.:+33-56-84-64-38

David **Ford**
Concordia University
Dept. of Computer Science
1455 de Maisonneuve Blvd. West,
Montreal, Québec H3G 1M8
Canada
kbkfe@vax2.concordia.ca
tel.:+1-514-848 3015

István **Gaál**
Kossuth Lajos Universität
Mathematisches Institut
P.O.Box 12
H-4010 Debrecen
Hungary
igaal@tigris.klte.hu
tel.:+36-52-31 66 66

Josef **Gebel**
Universität des Saarlandes
Fachbereich 9 - Mathematik
Postfach 151150
D-66041 Saarbrücken
Germany
sepp@math.uni-sb.de
tel.:+49-681-302 3297

George **Havas**
University of Queensland
Dept. of Computer Science
Queensland, 4072
Australia
havsa@cs.uq.oz.au
tel.:+61-7-365-29 04
afx +61-7-365-19 99

Mike **Jacobson**
University of Manitoba
Dept. of Computer Science
Winnipeg, Manitoba R3T 2N2
Canada
jacobs@silver.cs.umanitoba.ca
tel.:+1-204-269 9178

Valeri I. **Korjik**
Leningrad Electroengeneering
Institute of Communications
Moika 61
191065 St. Petersburg
Russia
bymey@iec.spb.su
tel.:+7-812-315 8247

Franx **Lemmermeyer**
Universität Heidelberg
hb3@ix.urz.uni-heidelberg.de
Erwin Rohde-Straße 19
69120 Heidelberg

Arien K. **Lenstra**
Bellcore – Morristown
Bellcore
Rm.2Q-334
445 South St., P.O.Box 1510
Morristown, NJ 07962-1910
USA
lenstra@bellcore.com
tel.:+1-201-829-48 78

R. **Lercier**
Ecole Polytechnique
LIX
BP 105
F-91128, Palaiseau, CEDEX
France
lercier@poly.polytechnique.fr
tel.:+33-1-69 33 45 89

Jacques **Martinet**
Université Bordeaux I
UFR de Mathémathiques et
Informatique
351 Cours de la Libération
F-33405, Talennce, Cedex
France
martinet@ceremab.u-bordeaux.fr
tel.:+33-56-84-60-96

Alfred **Menezes**
University of Aubern
120 Math Annex
Auburn, AL 36849
USA
menezal@mail.auburn.edu
tel.:+1-205-844-36 44

Victor S. **Miller**
CCR – Pricetown
29 Thanet RD
Princetown, NJ 08540
USA
victor@ccr-p.ida.org
tel.:+1-609-924-46 00

Francois **Morain**
Ecole Polytechnique
LIX
BP 105
F-91128, Palaiseau, CEDEX
France
morain@poly.polytechnique.fr
tel.:+33-1-69 33 45 89

Volker **Müller**
Universität des Saarlandes
Fachbereich 14 - Infornatik
Postfach 151150
D-66041 Saarbrücken
Germany
vmueller@cs.uni-sb.de
tel.:+49-681-302 4157

Ken **Nakamula**
Tokyo Metropolitan University
Dept. of Mathematics
Minmi-Ohsawa 1 - 1
Hachoji-shi
Tokyo, 192-03
Japan
nakamula@math.metro-u.ac.jp
tel.:+81-426-77-24 71

Harald **Niederreiter**
Österreichische Akad.
der Wissenschaften
Institut f‘”ur
Informationsverarbeitung
Sonnenfelsgasse 19
A-1010 Wien
Austria
nied@qiinfo.oeaw.ac.at
tel.:+43-1-51581 320

Andrew M. **Odlyzko**
AT & T Bell Labs.
Room 2C-355
600 Mountain Av.
Murray Hill, NJ 07974
USA
amo@research.att.com
tel.:+1-908-582-7286

Tatsuaki **Okamoto**
AT & T Bell Labs.
Room 2D-301
600 Mountain Av.
Murray Hill, NJ 07974
USA
okamoto@research.att.com

Michel **Olivier**
Université Bordeaux I
UFR de Mathémathiques et
Informatique
351 Cours de la Libération
F-33405, Talennce, Cedex
France
olivier@ceremab.u-bordeaux.fr
tel.:+33-56-84-61-02

Attila **Pethö**
Medical University Debrecen
Lab for Informatics
Nagyerdei krt. 98
H-4028 Debrecen
Hungary
pethoe@peugeot.dote.hu
tel.:+36-52-43 15 00

Alf **van der Poorten**
Macquarie University Sidney
School of MPCE
Sidney, NSW 2109
Australia
alf@mpce.mq.edu.au
tel.:+61-2-850-9500

Michael **Pohst**
TU Berlin
Fachbereich 3 Mathematik
sek. Ma 8-1
Straße des 17. Juni 136
D-10623 Berlin
pohst@math.tu-berlin.de
tel.:+49-30-314 257 72

Jean-Jacques **Quisquater**
Université de Louvain
FAI – Dept. of Electrical
Engeneering
Place du Levant 3
B-1348 Louvain-la-Neuve
Belgium
jiq@dice.ucl.ac.be
tel.:+32-1047-2541

Herman **Te Riele**
CWI - Amsterdam
CWI – Mathematisch Centrum
Kruislaan 413, Postbus 94079
NL-1090 GB Amsterdam
The Netherlands
herman@cwl.nl
tel.:+31-20-592-41 06

Oliver **Schirokauer**
Oberlin College
Dept. of Mathematics
Oberlin, OH 44074
USA
oliver@pekochan.math.oberlin.edu

Renate **Scheidler**
University of Delaware
Dept. of Mathematical Sciences
Newark, DE 19716
USA
scheidle@math.udel.edu
tel.:+1-302-831-18 83

Claus P. **Schnorr**
Universität Frankfurt
Fachbereich Mathematik
Robert Mayer-Straße 6 – 10,
PF 11 19 32
D-60054 Frankfurt
schnorr@informatik.uni-frankfurt.de
tel.:+49-69-798 2526

Wolfgang **Schwarz**
Universität des Saarlandes
Fachbereich 9 - Mathematik
Postfach 151150
D-66041 Saarbrücken
Germany
sepp@math.uni-sb.de
tel.:+49-681-302 3297

Victor **Shoup**
Universität des Saarlandes
Fachbereich 14 - Infornatik
Postfach 151150
D-66041 Saarbrücken
Germany
shoup@cs.uni-sb.de

Igor **Shparlinski**
Macquarie University Sidney
School of MPCE
Sidney, NSW 2109
Australia
igor@mpce.mq.edu.au
tel.:+61-2-805-9574

Roel **Stroeker**
Erasmus University Rotterdam
Econometric Institute
P.O.Box 1738
NL-3000 FDR Rotterdam
The Netherlands
stroeker@wis.few.eur.nl
tel.:+31-10-408-12 60

Nigel P. **Smart**
University of Wales
Dept. of Computer Science
College of Cardiff
Cardiff CF2 4A9
Great Britain
nigel.smart@cm.cf.ac.uk

Chris **Smyth**
University of Edinburgh
Dept. of Mathematics
King's Building
Mayfield Road
Edinburgh EH9 3JZ
Great Briatin
chris@mathematics.edinburgh.ac.uk
tel.:+44-31-650-50 54

Nikos **Tzanakis**
University of Crete
Dept. of Mathematics
P.O.Box 14 70
GR-714 09 Iraklion, Crete
Greece
tzanakis@talos.cc.uch.gr
tel.:+30-81-232-9 62

Benjamin M.M. **de Weger**
Erasmus University Rotterdam
Econometric Institute
P.O.Box 1738
NL-3000 FDR Rotterdam
The Netherlands
dweger@wis.few.eur.nl
tel.:+31-10-408-1438 / 2231

Susanne Wetzel
Universität des Saarlandes
Fachbereich 14 - Infornatik
Postfach 151150
D-66041 Saarbrücken
Germany
swetzel@acm.org

Brigitte **Vallée**
Université de Caen
LAIAC
F-14032 Caen, CEDEX
France
brigitte.vallee@univ-caen.fr
tel.:+33-31 45 56 57

Horst Günther **Zimmer**
Universität des Saarlandes
Fachbereich 9 - Mathematik
Postfach 151150
D-66041 Saarbrücken
Germany
zimmer@math.uni-sb.de
tel.:+49-681-302 2206