Johannes Buchmann, Harald Niederreiter,
Andrew M. Odlyzko, Horst G. Zimmer (editors):

Algorithms and Number Theory

Dagstuhl-Seminar-Report; 39
22.06.-26.06.92 (9226)

ISSN 0940-1121

Das Internationale Begegnungs- und Forschungszentrum für Informatik (IBFI) ist eine gemeinnützige GmbH. Sie veranstaltet regelmäßig wissenschaftliche Seminare, welche nach Antrag der Tagungsleiter und Begutachtung durch das wissenschaftliche Direktorium mit persönlich eingeladenen Gästen durchgeführt werden.

Verantwortlich für das Programm:
Prof. Dr.-Ing. José Encarnaçao,
Prof. Dr. Winfried Görke,
Prof. Dr. Theo Härder,
Dr. Michael Laska,
Prof. Dr. Thomas Lengauer,
Prof. Ph. D. Walter Tichy,
Prof. Dr. Reinhard Wilhelm (wissenschaftlicher Direktor)

Gesellschafter: Universität des Saarlandes,
Universität Kaiserslautern,
Universität Karlsruhe,
Gesellschaft für Informatik e.V., Bonn

Träger: Die Bundesländer Saarland und Rheinland-Pfalz

Bezugsadresse: Geschäftsstelle Schloß Dagstuhl
Informatik, Bau 36
Universität des Saarlandes
W - 6600 Saarbrücken
Germany
Tel.: +49 -681 - 302 - 4396
Fax: +49 -681 - 302 - 4397
e-mail: office@dag.uni-sb.de

Dagstuhl Workshop
on
Algorithms and Number Theory

June 22 - 26, 1992

Organizers:

Johannes Buchmann (Saarbrücken)
Harald Niederreiter (Wien)
Andrew M. Odlyzko (New Jersey)
Horst Günter Zimmer (Saarbrücken)

Overview

The main interest of this workshop was the theory and practice of algorithms in number theory. The conference covered algorithms for factoring integers and polynomials, discrete logarithms, quadratic forms, diophantine equations, elliptic and hyperelliptic curves, and number fields.
The 35 participants of this workshop came from 10 countries. Besides the formal program, there was ample time for free discussions and informal meetings between participants. The nice setup of the Dagstuhl Institute made this workshop a very enjoyable experience.

The organizers would like to thank everyone who contributed to the success of this meeting.

ABSTRACTS

On the Analogue of the Division Polynomials for Hyperelliptic Curves

David G. Cantor

We study hyperelliptic curves given by Weierstrass equations of the form

$$Y^2 = F(X) = \sum_{i=0}^{2g+1} a_i X^i, \quad a_{2g+1} = 1.$$

When $g = 1$ these are elliptic curves. In this case, there are well-known division polynomials which can be used to multiply a point by an integer r.

When g is > 1, then one must work with the Jacobian of this curve. We obtain the analogue of the division polynomials. These can be used to determine the cardinality of the Jacobian.

A Deterministic Factorization Algorithm for Polynomials over Finite Fields

Harald Niederreiter

Let $\mathbb{F}_q$ be a finite field of order q (q an arbitrary prime power), $f \in \mathbb{F}_q[x]$ a monic squarefree polynomial with $deg(f) = d \geq 1$, and $g_1, ..., g_m \in \mathbb{F}_q[x]$ the distinct monic irreducible factors of f. Consider the differential equation

$$f^q H^{(q-1)}\left(\frac{h}{f}\right) = h^q \tag{1}$$

with unknown $h \in \mathbb{F}_q[x]$, where $H^{(q-1)}$ is the Hasse-Teichmüller derivative of order $q-1$. Then (1) has a linear solution space with an $\mathbb{F}_q$-basis given by $\frac{f}{g_i}g_i', 1 \leq i \leq m$. Moreover, (1) is equivalent to a $d \times d$ homogeneous system of linear equations for the coefficients of h. By calculating $\gcd(f, h)$ for all solutions h of (1), we get all monic factors of f (with repetitions if $q > 2$). In the case $q = 2$ this method simplifies considerably. First of all, (1) reduces to the ordinary differential equation

$$(fh)' = h^2. \tag{2}$$

Furthermore, (2) is equivalent to a $d \times d$ system of linear equations for the coefficients of h with no set-up cost (as opposed to the set-up cost $O(d^2)$ in the Berlekamp algorithm). If f is sparse, then the system of linear equations is sparse. Also, the system has a very special structure which may allow faster solution methods.

Some New Results from Numerical Sieving Devices

Hugh C. Williams

A machine is called a number sieve if it is a device which finds solutions to systems of single variable linear congruences with varying moduli. The mechanism detects these solutions by simple searching through all the integers up to a certain bound. In this paper, we discuss the results of running this type of device on two different problems. The first of these is the difficult problem of tabulating $g(k)$, where $g(k)$ is the least positive integer such that all prime divisors $g\binom{g(k)}{k}$ must exceed $k+1$. By using the OASIS system at the university of Manitoba, we were able to produce an extensive list of all values of $g(k)$ for $2 \leq k \leq 151$, with the exception of $g(150)$ only.

The second problem is that of determing pseudoprimes. Let p be an odd prime; a pseudoprime $< p$ is the least positive integer which is not a perfect square such that $L_p \equiv 1 \ (mod\ 8)$ and $(L_p/g) = 1$ for all primes $g \leq p$. By developping a new sieve which makes use of 16 of the SSU VLSI sieve chips designed by Cam Patterson, we were able to search through the integers for pseudoprimes at the rate of about 8.9×10^{11} per second. As a result of running this device for a few weeks, we now know all the pseudoprimes up to and including L_{239}. These numbers are of particular interest because of their connection to the problem of whether primality testing is in complexity class $\mathbb{P}$.

Computing Resolvents and Galois groups for polynomials with small degree

Michel Olivier

Let $f(x) \in \mathbb{Z}[x]$ be monic irreducible. We want to compute the Galois group of f. We describe an algorithm for computing relative H-polynomials to G, where H and G are transitive subgroups of S_n of degree n, such that $H \subset G$.

$P(x_1, ..., x_n)$ is a relative H-polynomial to G if

$$H = \{\sigma \in G : \sigma P = P\}.$$

The resolvent relative to G, H, P and f is

$$R(x) = \prod_{\tau} (x - \tau P(\theta_1, ..., \theta_n)),$$

where τ runs over a complete representative set of G mod H, $P(x_1, ..., x_n)$ is a relative H-polynomial to G, $f(x) \in \mathbb{Z}[x]$ is a monic irreducible polynomial, and $(\theta_1, ..., \theta_n)$ are the roots of f in $\mathbb{C}$.

We give the graph of all transitive groups with degree 8 and 9, and all resolvents needed for computing the Galois group of f.

Massively Parallel Computation of Discrete Logarithms

Kevin McCurley

The discrete logarithm problem is the following: given group elements a and g, find an integer x such that $g^x = a$, provided such an x exists. This problem arises in cryptography from trying to invert the presumed one-way-function $f(x) = g^x$. We have (joint with Dan Gordon) now completed most of the computation required to compute discrete logarithms in the multiplicative group of $GF(2^{401})$ and $GF(2^{503})$. The algorithm that we are using is based on that of Coppersmith, but we use a sieving method to screen polynomials over $GF(2)$ for divisibility by irreducibles of small degree. In the second phase of the computation we have used a massively parallel MIMD implementaion of the conjugate gradient algorithm for solving linear systems over finite fields. All of this work was performed on large MIMD machines, including two 1024 processors nCUBE-2 hypercubes with 4 GB of RAM, and Intel iPSC 860 with 64 processors, and the Ddta Touchstone Intel mesh-connected machine with 512 processors. The linear algebra phase involves solving a sparse system of approximately 10000 - 80000 equations over a field $GF(p)$ where p is 100-500 bits.

Iterated absolute values of differences of consecutive primes

Andrew M. Odlyzko

Let $p_1 = 2,\ p_2 = 3, \ldots$ be the primes, and set

$$\begin{array}{rcll} d_0(n) & = & p_n, & n \geq 1 \\ d_k + 1(n) & = & |d_k(n) - d_k(n+1)|, & n \geq 1,\ k \geq 0. \end{array}$$

A conjecture, usually ascribed to Gilbreath, but actually due to Proth in the 19-th century says that $d_k(1) = 1$ for all $k \geq 1$. This conjecture has now been verified numerically for $k \leq \pi(2 \times 10^{12}) \approx 2 \times 10^{10}$. The numerical evidence supports heuristic arguments, that this conjecture is true for many other sequences as well that are sufficiently nicely behaved.

Block Korkin-Zolotarev Bases and Succesive Minima

Claus-Peter Schnorr

Let $b_1, \ldots, b_m \in \mathbb{R}^n$ be a basis of lattice L that is a block Korkin-Zolotarev basis with block size β and let $\lambda_i(L)$ denote the successive minima of lattice L. We prove that

$$\frac{4}{i+3}\,\gamma_\beta^{-\frac{2i}{\beta-1}} \;\leq\; \|b_i\|^2/\lambda_i(L)^2 \;\leq\; \gamma_\beta^{\frac{2m}{\beta-1}}\,\frac{i+3}{4} \quad \text{for } i = 1, \ldots, m$$

where γ_β is the Hermite constant. For $\beta = 3$, we establish the optimal upper bound

$$\|b_1\|^2/\lambda_1(L)^2 \leq \left(\frac{3}{2}\right)^{\frac{m-1}{2}-1}$$

and we present block Korkin-Zolotarev lattice bases achieving this bound.

We improve the NEAREST PLANE ALGORITHM of BABAI (1986) using block Korkin-Zolotarev basis. Given a block Korkin-Zolotarev basis $b_1, \ldots, b_m$ with block size β and $x \in L(b_1, \ldots, b_m)$, a lattice point v can be found in time $\beta^{O(\beta)}$ satisfying $\|x - v\|^2 \leq m\gamma_\beta^{\frac{2m}{\beta-1}} \min_{u \in L} \|x - u\|^2$.

Factoring with ECM

Franz-Dieter Berger

There are several ways to implement the elliptic curve method (ECM). I talked about my practical experience with

- simultaneous gcd computation
- standard continuation
- improved standard continuation

(suggested by Montgomery, 1987)

- parallel implementation using a UNIX network.

It turns out that the theoretical speedup of the simultaneous gcd method is in practice not reachable and that the improved standard continuation is preferable, if you have enough main memory.

Massively Parallel Factoring

Arjen K. Lenstra

In joint work with Brandon Dixon (Princeton University) and Dan Bernstein (University of Berkley), we did some experiments with Single Instruction Multiple Data (SIMD) implementations of several integer factoring methods: elliptic curve method (ecm), double large prime multiple polynomial quadratic sieve (ppmpqs), and the lattice sieve variant of the number field sieve (lnfs). On a 16K MasPar SIMD computer, which consists of 16384 small (0.2 mips) processors on a 128 * 128 grid, this led to the following results:

- the first ever found 40 digit ecm factor, using a program that runs 1280 curves in parallel on 16384 processors and that makes use of a new version of Montgomery multiplication,
- the factorization of the 110-digit number on the RSA challenge list using ppmpqs in 30 days of CPU time, and
- an implementation of lnfs that would need slightly more than one week of CPU time to factor F_9.

Experiences with Pomerance's self-initializing quadratic sieve method on a Cray Y-MP4

Herman te Riele

We have implemented Pomerance's self-initializing version of the quadratic sieve factoring algorithm on the Cray Y-MP4 supercomputer of the Academic Computer Center (SARA) in Amsterdam. For 81-digit numbers and for the polynomials in the above factoring algorithm having a leading coefficient which is the square of four distinct prime factors, we found a reduction of the CPU time spent in the initialization of the polynomials of about 0.5. However, since this polynomial initialization time consumes only about 8% of the total CPU time, the time to factor the number was reduced only by a factor of about 0.96. We expect this reduction factor to become about 0.92 for an implemetation of Pomerance's self-initializing quadratic sieve algorithm on a Silicon Graphics workstation (if sufficient memory is available).

On the analytic rank in families of twists of elliptic curves

Gerhard Frey

Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N_E. We assume that E is modular and hence its L-series, $L_E(s) = \sum a_n n^{-s}$, has an analytic continuation to the complex plane and satisfies a functional equation. For a squarefree integer D prime to E, the twist E_D of E has an L-series $L_{E_D}(s) = \sum \chi_D(n) a_n n^{-s}$ and, due to the results of Gross-Zagier, Kolyvagin and others, the set of $\mathbb{Q}$-rational points of E_D is finite, if $L_{E_D}(1) = 0$, otherwise the (analytic) rank of E_D is positive. If E_D is even (i.e. $L_E(s)$ is an even function), one can compute

$$L_{E_D}(1) = \sum \chi(n) \, \frac{a_n}{n} \quad \frac{2\pi n}{e^{|D|\sqrt{N_E}}},$$

and we are interested in the set of numbers D with $L_{E_D}(1) = 0$. Using a theorem of Waldspurger, one can translate this equation into an analogous question about Fourier coefficients of a cusp form F_E of weight $3/2$ which is mapped to $f_E(t) = \sum a_n e^{2\pi i n z}$ by the Shimura map. We determined F_E in some curves (for instance for the curves 11B, 19B, 38B, 49A, 98B of the Antwerp tables) and computed its Fourier coefficients up to $n \approx 3 \cdot 10^6$. It turned out that, in all cases, the ratio of the number of twists E_D with positive rank divided by all twists $E_D (0 < D \leq n)$ is behaving like $\frac{1}{(\log n)^2 \log\log n}$.

Class groups and selmer groups

Edward Schaefer

It is often the case that a selmer group of an Abelian variety and a group related to an ideal class group can be embedded into the same group of homomorphisms.

Ideally the images of the two groups are almost the same so we can get information about one group from the other. In order to do this, we compute upper bounds on the index of the intersection in each of the two groups. We do this by computing locally where we have quick algorithms for elliptic curves and good ideas for abelian varieties in general.

The Discrete Logarithm at Jacobians of Algebraic Curves

Hans-Georg Rück

For the development of cryptosystems based on exponentiation one needs finite abelian groups in which the evaluation of the discrete logarithm is a difficult problem. We consider jacobians of algebraic curves over finite fields. Examples for these curves are elliptic and hyperelliptic curves. We present explicit formulas for the addition law on their jacobians. This leads to a "Schoof-Algorithm" for curves of genus 2 (Thesis W. Kamphätter).
Furthermore, we state a general theorem (joint work with G. Frey) which shows that in certain cases the evaluation of the discrete logarithm in jacobians can be reduced to the evaluation of the discrete logarithm in the multiplicative group of a finite field. Hence in order to find curves whose jacobians are useful for cryptosystems, one must avoid the assumptions of this theorem.

The Demjanenko matrix - a link between torsion points on elliptic curves and units in cyclotomic fields

Horst G. Zimmer

In proving the boundedness conjecture for the class of 2-deficient elliptic curves E over a number field K, H. G. Folz encountered the **Demjanenko matrix** D over the prime field $\mathbb{F}_2$. For a prime $p \geq 5$, one considers the set $M = (\mathbb{Z}/p\mathbb{Z})^* \cap \{\overline{1}, \overline{2}, ..., \overline{\frac{p-1}{2}}\}$ of cardinality $m = \frac{p-1}{2}$ and takes its characteristic function

$$\chi_M : ({}^{\mathbb{Z}}\!/_{p\mathbb{Z}})^* \to \{0, 1\}$$

to define

$$D = (\chi_M(i \cdot j))_{i,j \in M} \in \mathbb{F}_2^{m \times m}.$$

In general, D has **rank**

$$\varphi = rk_{\mathbb{F}_2} D = \frac{p-1}{2} - d$$

with **defect** $d = 0$, but there are primes p for which the defect is $d > 0$; e.g., $p = 29, 113$ and 163, where $d = 3, 3$ and 2, respectively. Those primes p having defect $d > 0$ are called **exceptional**. Folz found a stronger bound for the torsion primes p that are non-exceptional than for exceptional torsion primes.
On the other hand, let $K = \mathbb{Q}(\xi)$ denote the p-th cyclotomic field and $K^+ = \mathbb{Q}(\xi + \xi^- 1)$ its maximal real subfield. Let h and h^+ stand for the **class number** and E and E^+ for the **unit group** of K and K^+ respectively. Consider the subgroup $E_{cyc} \leq E$ of cyclotomic units of K and the corresponding subgroup $E_{cyc}^+ \leq E^+$ with respect to K^+, where $E_{cyc}^+ = E_{cyc} \cap K^+$, and introduce the subgroup $E_{cyc}^{pos} \leq E_{cyc}^+$ of totally positive cyclotomic units in K as well as the subgroup $E^{pos} \leq E^+$ of arbitrary totally positive units in K^+. As usual, let $h^- = h/h^+$, the minus part of the class number h of K. Combining results of E. Reyssat and F. Hazama, W. Schwarz proved the following
Theorem The following are equivalent:

1. D is singular over $\mathbb{F}_2$, i.e. $d > 0$;
2. $2|h^-$;
3. $(E_{cyc}^{pos} : E_{cyc}^{+2}) > 1$;
4. $2|h^+$ or $(E^{pos} : E^{+2}) > 1$.

Some numerical experiments showed that the defect of the Demjanenko matrix D is

$d \leq 4$ for $p < 1000$ (Folz)

$d \leq 12$ for $p < 10000$ (M. Klar)

$d \leq 15$ for $p < 100000$ (Schwarz).

These results suggest that

$$\limsup_{p \to \infty} \frac{d}{\log_2 p} \geq 1.$$

Short representation of numbers in number fields

Johannes Buchmann

I tried to prove:

Theorem

Let K be an algebraic number field of absolute discriminant D. For each integer α in K, there is a representation

$$\alpha = \prod_{i=1}^{l} \alpha_i^{e_i}$$

such that

$$\begin{aligned} |\alpha_i|_s &\leq \max\{\log D, \log N(\alpha)\}^{O(1)} \\ l, \log e_i &\leq (\log\log H(\alpha))^{O(1)}, \end{aligned}$$

where $|\ |_s$ denotes the binary length of an appropriate basis representation.

On the resolution of index form equations in quartic number fields

Istvàn Gaàl

Let $K = \mathbb{Q}(\xi)$be a quartic number field generated by the element ξ with $I(\xi) = n$ and defining polynomial $f(x) = x^4 + px^3 + qx^2 + rx + s$. Furthermore, let g be an integer, such that any $\alpha \in \mathbb{Z}_K$ can be written in the form $\alpha = (x_1 + x_2\xi + x_3\xi^2 + x_4\xi^3)/g$, with $x_1, x_2, x_3, x_4 \in \mathbb{Z}$.

Theorem

$\alpha \in \mathbb{Z}_K$ has index m if and only if there is a solution $(M, N) \in \mathbb{Z}^2$ of

$$F(M, N) = \frac{g^6 m}{n} \tag{1}$$

such that there exist $(x_2, x_3, x_4) \in \mathbb{Z}^3$ with

$$\begin{aligned} Q_1(x_2, x_3, x_4) &= M \\ Q_2(x_2, x_3, x_4) &= N, \end{aligned} \tag{2}$$

where $F \in \mathbb{Z}[X,Y]$ is a binary cubic form, $Q_1, Q_2 \in \mathbb{Z}[x_2, x_3, x_4]$ are ternary quadratic forms, all of them having coefficients depending only on p, q, r, s.

Equation (1) is either trivial to solve (if F is reducible) or (1) is a cubic Thue equation that can also be solved without difficulties. We give a general method, applicable to any quartic field, to find the solutions with $\max |x_i| < 10^{10}$ of (2). Moreover, in case of totally complex quartic fields, we can determine all solutions of (2) by using the following statement:

Theorem
If K is totally complex, then $F(x,1) = 0$ has three distinct real roots, $\lambda_1 < \lambda_2 < \lambda_3$. The form

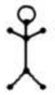
$$Q_1(x_2, x_3, x_4) + \lambda Q(x_2, x_3, x_4)$$

is a positive definite quadratic form if and only if $\lambda \in (\lambda_1, \lambda_2)$.

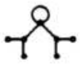
Children's drawings - dessins d'enfant

Hendrik W. Lenstra

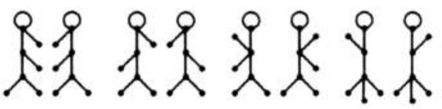
In this lecture, I attempted to explain what people mean when they say that a drawing like



gives rise to a number field $K \subset \mathbb{C}$ that has degree 10 over $\mathbb{Q}$, that has 2 real places and 4 complex places, and that is unramified at all primes $p > 14$. The number 10 is the total number of "conjugates" of the drawing, which are two symmetric ones - the drawing itself and



and from pairs of asymmetric ones:



The number 14 is twice the number of edges in the drawing.

The lecture gave not much more than definitions. They depend on a theorem that describes all unramified coverings of $\mathbb{P}^1(\mathbb{C}) - \{0, 1, \infty\}$, and which depends on algebraic topology and the Riemann existence theorem.

All that is known so far in the theory of children's drawings has been known, in substance, for a long time. It is hoped that a better understanding will lead to more information on the absolute Galois group of $\mathbf{Q}$. This hope is due to Grothendieck, but, with possible exception of him, nobody seems to know where the theory is going. For this reason, many numerical experiments one performed, and they led to results that the theory cannot yet fully explain.

Computation of Grothendieck dessins

Henri Cohen

In this talk, we explain algorithms for computing the Belyi function φ of a Grothendieck dessin (see H. Lenstra's talk). They involve in particular the extensive use of Groebner bases algorithms or, at best, of resultants. The special cases of trees is mentioned for which a simple combinatorial formula allows us to deduce the degree of the number field in many cases.
The special cases of quadratic and cubic fields is mentioned. Finally, the case of the dessin (not a tree) is described.

Progress on Thue equations

Benne de Wegner

(1) A general procedure for solving Thue equations $F(X,Y) = m(F \in \mathbb{Z}[X,Y],\ m \in \mathbb{Z})$ in $X, Y \in \mathbb{Z}$ was described by Tzanakis & de Wegner in 1989. This procedure requires explicit knowledge of a system of fundamental units of the field $L = \mathbf{Q}(\vartheta)$ defined by $F(\vartheta, 1) = 0$. It is shown that it suffices to know only the independent units, at least when $m = 1$, at the cost of a tiny amount of extra computations.

(2) The procedure is generalized to Thue equations over rings of integers. That is, when K is an algebraic number field, we consider $F \in O_K[X,Y], m \in O_K$. The most important observation here is that one needs relative units over K of L. A consequence is that a Thue equation over $\mathbb{Z}$, for which L has a proper subfield of index ≥ 3, is easier to solve than an arbitrary Thue equation of the same degree.

(3) The p-adic Mordell equations

$$\begin{aligned} y^2 - x^3 &= \pm 2^a 3^b 5^c 7^d, \\ y^2 - x^3 &= \pm 2^a 3^b 11^c \end{aligned}$$

can be reduced to:

- 22 cubic equations,
- 122 cubic Thue-Mahler equations (with ≤ 3 primes)
- the equation $u + v = \square$, with u, v having only 2, 3, 5, 7 (resp. 2, 3, 11) as prime divisors.

All these equations can be solved completely and the plan is to actually do so in the near future.

(1) joint work with N. Tzanakis
(2) joint work with N. Smart

Divisibility properties of solutions of a diophantine equation

Herman te Riele

Based on congruences mod p, for prime p, and on properties of Bernoulli polynomials and Bernoulli numbers, several conditions are derived for $x, k \geq 2$ if they satisfy the diophantine equation

$$1^k + 2^k + ... + (x-1)^k = x^k.$$

Using the results of experiments with these conditions on a Silicon Graphics' workstation, it is proved that x is neither divisible by a regular prime, nor by any irregular prime < 10000 and that k is divisible by the least common multiple of all the positive integers ≤ 210. The results obtained indicate that it is just a matter of spending more CPU-time to extend these results.

(joint work with Pieter Moree and Jezzy Urbanowiez)

Generalization of the Voronoi algorithm for quadratic forms

Jacques Martinet

A quadratic form Q on $\mathbb{R}^n$ is said to be **perfect** when the matrices $P_X = X\,{}^tX$ span $\mathrm{sym}_n(\mathbb{R})$ for $X \in S(Q)$, the set of minimal vectors of $\mathbb{Q}$ (for $X \in \mathbb{Z}^n$). Voronoi defined **the domain $\mathcal{D}_Q$ of Q** in $\mathrm{sym}_n(\mathbb{R})$, a convex polyedral cone, and attached to each face $\mathcal{F}$ of $\mathcal{D}_Q$ a new perfect form; this defines a graph.

Theorem
This graph is connected and the quotient graph for forms up to equivalence (and scaling) is finite.

We generalize this result of Voronoi by introducing the notion of a **T-perfect form** for convenient subspaces T of sym_n and the notion of T-equivalence and prove a theorem of convexity. This can be applied for forms invariant under a given integral representation with

$$\mathcal{T} = \{M \in \mathrm{sym}_n |\ \forall s \in G,\ {}^t\!\rho(s) M \rho(s) = M\}$$

or for forms with given form $Q(x_1, \ldots, x_r, 0, \ldots, 0)$.

Joint work with Anne-Marie Bergé (Bordeaux) and François Sigrist (Neuchâtel), to appear in Astérisque.

On integral lattices of prescribed minimum

Michael E. Pohst

We report on joint work with W. Plesken (Aachen). For $m = 2, 3, 4$ we computed all ascending chains of lattices $\Lambda_1 \subseteq \Lambda_2 \subseteq \ldots$ in Euclidean space with the properties

i) Λ_i is of dimension i,

ii) Λ_i is integral,

iii) $m = M(\Lambda_i) := \min\{\|\underline{x}\|^2 | \underline{x} \in \Lambda_i - \{\underline{0}\}\}$,

iv) Λ_i is generated by vectors of length m,

v) Λ_{i+1} is of minimal discriminant among all lattices satisfying (i)-(iv) (for $i+1$) and containing Λ_i.

In the sequel, we only describe the (new) results for $m = 4$. Then all lattices up to dimension 24 lie in the Leech lattice L. Hence, for $i > 24$ we have $\Lambda_i = L \perp \Gamma_{i-24}$ for some lattice Γ_{i-24} which again satisfies (i) - (v). Besides the lattices themselves, we computed all their vectors of minimal length and their automorphism groups.

DANFI, a data base for algebraic number theory

Attila Pethö

I reported on the database DANFI which is developed by Katalin Boguár (Debrecen) and Ulrich Schröter (Düsseldorf). With the help of DANFI one can get reports and views on characteristic data of algebraic number fields. A special feature of the database is that it will work closely connected with the software package KANT developed in Düsseldorf.

Squares in recurrence sequences

Attila Pethö

We gave in this lecture an outline of the proof of the following theorem:

Let $\varepsilon, \varepsilon_1 \in \{1, -1\}$. Assume that there exist a cyclic cubic number field K and an $\eta \in \mathbb{Z}_K$ such that

$$\begin{aligned} N_{K/Q}(\eta) &= \varepsilon \\ N_{K/Q}(\eta^2 - 11\eta - 1) &= \varepsilon_1 5^n \end{aligned}$$

holds for a $n \in \mathbb{Z}_{\geq 0}$. Then K is generated by one of the polynomials

$$\begin{array}{ccccccc}
z^3 & - & 12z^2 & + & 9z & + & 1 \\
z^3 & - & 12z^2 & + & 35z & + & 1 \\
z^3 & + & 3z^2 & - & 160z & + & 1 \\
z^3 & - & 17z^2 & - & 25z & + & 1 \\
z^3 & - & 13z^2 & + & 10z & + & 1 \\
z^3 & - & 14z^2 & + & 11z & + & 1 \\
z^3 & - & 9z^2 & + & 6z & + & 1 \\
z^3 & + & 3z^2 & - & 10z & + & 1
\end{array}$$

and η is one of their zeros. The converse is also true.

Computations in number fields

Francisco Diaz y Diaz

I describe some simple computations on relative discriminants of number fields extensions and I show how to use it to simplify the proof of the existence of non-isomorphic number fields having the same discriminant and the possible existence of unessential divisors of the relative discriminant on related topics.
The paricular examples considered here come from the tables of unprimitive number fields of degree nine computed by M. Olivier and myself.

Addition laws on elliptic curves

Wieb Bosma

An addition law on an elliptic curve: $E : Y^2Z = X^3 + AXZ^2 + bZ^3$ consists of a triple of polynomials x_3, y_3, z_3 in $\mathbb{Z}[A, B][x_1, y_1, z_1,\ x_2, y_2, z_3]$ such that not all three are zero and on same open, nonzero subset $U \subseteq E \times E$ one has

$$(x_1 : y_1 : z_1) + (x_2 : y_2 : z_2) = (x_3 : y_3 : z_3).$$

By elementary methods one easily arrives at a triple of addition laws for which the defining opens cover $E \times E$ (a **complete** system). The bidegree of these formulars

will be (2,2), (3,3), (9,9) respectively. In a paper by H. Lange & W. Ruppert, it was proved (Invent. Math. 1985) that there exists a complete system of addition laws of bidegree (2,2). Moreover, they exhibit a complete system of 3 such laws.
Using these, it is proved in this talk that there exists a complete system of 2 addition laws of bidegree (2,2).

Fast exponentiation with precomputation

Kevin McCurley

The computational problem of computing g^n for large n and g in some group is one that arrises in many cryptographic systems based on the discrete logarithm problem. For the RSA system, the problem that arises has n fixed, and g, depending as it does on the message, varies across the reduced residues modular a large composite. By contrasts in the Diffie-Hellman, El Gamal, and the newly proposed digital signature standard DSS, g remains fixed and n varies across a large range, typically 160 bits or 512 bits.
For fixed exponent n, the best method uses addition chains, and uses at least K multiplications in the group when the exponent has k bits. For the case of g fixed and n chosen randomly from $[0, n]$, we show that a precomputation of $\frac{\log N}{\log\log N}$ powers of g allows us to compute g^n for $0 < n < N$ in $O\left(\frac{\log N}{\log\log N}\right)$ group multiplications. We prove that this is asymptotically optimal and we derive concrete lower bounds for some values of N that occur in applications. Moreover, the method is extremely practical. For example, if N has 512 bit, then our method can compute g^n in at most 106 multiplications if we precompute and store 362 powers of g, and 93 multiplications if we precompute and store 650 values. We discovered a range of methods that give a time-space tradeoff where more storage will reduce the amount of computation even further. This example may be compared with the value of 512-1022 multiplications for the standard binary method on addition chains.
We also show how to parallelize the method, achieving $\log\log N$ multiplications on $O\left(\frac{\log N}{\log\log N}\right)$ processors. We also show how to use storage to improve over normal basis methods in $GF(p^k)$, where raising to the p-th power is a cyclic shift and therefore almost free.

(Joint work with E.F. Brickel, D. Gordon, D. Wilson.)

Simultaneous unit and class group computation - practical experience

Johannes Graf von Schmettow

The most promising method for fast computation of the unit group and class group of an algebraic number field of arbitrary degree seems to be the "Relation method". We report on the progress being made in Düsseldorf when implementing it. This is done by using the number theory package KANT-2 which is written in Standard-C and uses the memory management, integer, real and polynomial features of the Cayley Platform. KANT-2 is public domain and will be available from October 1992.
The main idea of the relation method is to compute a factor basis consisting of prime ideals of the number field and then looking for relations among them, i.e. algebraic numbers that decompose into the given basis. Refined methods for enumerating lattice points within ellipsoids are needed for finding the relations.The resulting matrix of exponents is then Hermite-reduced. The columns consisting of 0's represent units - using reduction techniques of lll-type it is possible to compute a basis of the given units, even if the unit rank is comparativly large.
The structure of the class group can also be derived from the Hermite normal form. Of course at the end it is necessary to prove that one actually computed class group and unit group (and not only sub- or supergroups). This is done by root extracting methods which have been developed in Düsseldorf in the past years.

The method has been successfully used for fields of degree up to 24 and of unit rank up to 17.

Editor: Franz-Dieter Berger (Saarbrücken)

Dagstuhl-Seminar 9226: Teilnehmerliste (update:26.06.92)

Franz-Dieter **Berger**
Universität des Saarlandes
Fachbereich 14 - Informatik
Im Stadtwald 15
W-6600 Saarbrücken 11
Germany
fberger@cs.uni-sb.de
tel.: +49-681-302 4167

Wieb **Bosma**
The University of Sydney
School of Mathematics & Statistics
Sydney NSW 2006
Australia
wieb@maths.su.oz.au
tel.: +61-2-692 3338

Johannes **Buchmann**
Universität des Saarlandes
Fachbereich 14 - Informatik
Im Stadtwald 15
W-6600 Saarbrücken 11
Germany
buchmann@cs.uni-sb.de
tel.: +49-681-302 4156

David G. **Cantor**
Univ. of California at Los Angeles
Department of Mathematics
Los Angeles CA 90024
USA
dgc@math.ucla.edu
tel.: +1-619-755-5909

Henri **Cohen**
Université Bordeaux I
UFR de Mathematiques et Informatique
351 Cours de la Libération
F-33405 Talence Cedex
France
cohen@alioth.greco-prog.fr

Ilaria **Del Corso**
Scuola Normale Superiore
Piazza dei Cavalieri 7
I-56126 Pisa
Italy

Francisco **Diaz y Diaz**
Université Bordeaux I
UFR de Mathematiques et Informatique
351 Cours de la Libération
F-33405 Talence Cedex
France
diaz@alkaid.greco-prog.fr
tel.: +33-56 84 64 38

Gerhard **Frey**
Univ. GH Essen
Institut für Experimentelle Mathematik
Ellernstr. 29
W-4300 Essen 1
Germany
MEM010@DE0HRZ1A.bitnet
tel.: +49-201-320 6459 (6457)

Istvàn **Gaàl**
Heinrich-Heine Universität
Mathematisches Institut
Universitätsstraße 1
D-4000 Düsseldorf 1
Germany

Guido **von der Heidt**
Philipps-Universität Marburg
Fachbereich Mathematik
Lahnberge
W-3550 Marburg
Germany

Erwin **Hess**
SIEMENS AG - ZFE IS
Zentralabt. Forschung und Entwicklung
Otto-Hahn-Ring 6
Postfach 83 09 53
W-8000 München 83
Germany
tel.:+49-89-636 41040

Max **Jüntgen**
Heinrich-Heine Universität
Mathematisches Institut
Universitätsstraße 1
D-4000 Düsseldorf 1
Germany
juentgen@ze8.rz.uni-duesseldorf.de
tel.: +49-211-311-3204

Gerhard **Larcher**
Universität Salzburg
Institut für Mathematik
Hellbrunnerstraße 34
A-5020 Salzburg
Austria
tel.: +43-662-8044 5323

Hendrik W. **Lenstra Jr.**
University of California at Berkeley
Department of Mathematics
Berkeley CA 94720
USA
hwl@math.berkeley.edu
tel.: +1-510-643 7857

Arjen K. **Lenstra**
Belcore
Room 2Q334
445 South Street
Morristown NJ 07962-1910
USA
lenstra@flash.bellcore.com
tel.: +1-201-829 4878

Jacques **Martinet**
Université Bordeaux I
UFR de Mathematiques et Informatique
351 Cours de la Libération
F-33405 Talence Cedex
France
martinet@alcor.greco-prog.fr
tel.: +33-56-84-60-96

Kevin **McCurley**
Sandia National Laboratories
P.O. Box 5800
Albuquerque NM 87185
USA
mccurley@cs.sandia.gov
tel.: +1-505-845 7378

Harald **Niederreiter**
Österreichische Akad. der Wissenschaften
Institut für 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 Avenue
Murray Hill NJ 07974
USA
amo@research.att.com
tel.: +1-908-582 7286

Michel **Olivier**
Université Bordeaux I
UFR de Mathematiques et Informatique
351 Cours de la Libération
F-33405 Talence Cedex
France
olivier@mizar.greco-prog.fr
tel.: +33-56 84 61 02

Attila **Pethö**
Kossuth Lajos University
Mathematical Institute
P.O. Box 12
4010 Debrecen
Hungary
h2988pet@ella.hu
tel.: +36-52-11600/5953

Michael E. **Pohst**
Heinrich-Heine Universität
Mathematisches Institut
Universitätsstraße 1
D-4000 Düsseldorf 1
Germany
pohst@ze8.rz.uni-duesseldorf.de
tel.: +49-211-311-2188

Hans-Georg **Rück**
GHS Essen
Inst. f. Experimentelle Mathematik
Ellernstr. 29
W-4300 Essen
Germany
MEM030@DE0HRZ1A.bitnet
tel.: +49-201-3206455

Werner **Schaal**
Philipps-Universität Marburg
Fachbereich Mathematik
Lahnberge
W-3550 Marburg
Germany
tel.: +49-6421-28 2008

Edward F. **Schäfer**
490 Easy Street #9
Mountain View CA 94043
USA
tel.: +1-415-940-1099

Johannes **Graf von Schmettow**
Heinrich-Heine Universität
Mathematisches Institut
Universitätsstraße 1
D-4000 Düsseldorf 1
Germany
schmetto@ze8.rz.uni-duesseldorf.de
tel.: +49-211-311-3204

Ursula **Schneiders**
Universität des Saarlandes
Fachbereich 9 - Mathematik
Im Stadtwald 15
W-6600 Saarbrücken 11
Germany
ursula@math.uni-sb.de
tel.: +49-681-302-2297

Claus-Peter **Schnorr**
Universität Frankfurt
Fachbereich Mathematik
Robert-Mayer-Str. 6-10
W-6000 Frankfurt 11
Germany
schnorr@informatik.uni-frankfurt.de
tel.: +49-69-798 2526

Rob **Versseput**
Vrije Universiteit Amsterdam
Mathematisch Instituut
Plantage Muidergracht 24
NL-1081 TV Amsterdam
The Netherlands
rob@fwi.uva.nl

Benne M.M. **de Weger**
Universieit Twente
Dept. of Applied Mathematics
Postbus 217
NL-7500 AE Enschede
The Netherlands
deweger@math.utwente.nl
tel.: +31-53 89 34 11

Hugh C. **Williams**
The University of Manitoba
Deptartment of Computer Science
Winnipeg Manitoba R3T 2N2
Canada
hugh-williams@csmail.cs.umanitoba.ca
tel.: +1-204-474 9935

Jörg **Zayer**
Universität des Saarlandes
Fachbereich 14 - Informatik
Im Stadtwald 15
W-6600 Saarbrücken 11
Germany
zayer@cs.uni-sb.de
tel.: +49-681-302 4166

Horst Günter **Zimmer**
Universität des Saarlandes
Fachbereich 9 - Mathematik
Im Stadtwald 15
W-6600 Saarbrücken 11
Germany
zimmer@math.uni-sb.de
tel.: +49-681-302 2206

Zuletzt erschienene und geplante Titel:

G. Farin, H. Hagen, H. Noltemeier (editors):
Geometric Modelling, Dagstuhl-Seminar-Report; 17, 1.-5.7.1991 (9127)

A. Karshmer, J. Nehmer (editors):
Operating Systems of the 90s and Beyond, Dagstuhl-Seminar-Report; 18, 8.-12.7.1991 (9128)

H. Hagen, H. Müller, G.M. Nielson (editors):
Scientific Visualization, Dagstuhl-Seminar-Report; 19, 26.8.-30.8.91 (9135)

T. Lengauer, R. Möhring, B. Preas (editors):
Theory and Practice of Physical Design of VLSI Systems, Dagstuhl-Seminar-Report; 20, 2.9.-6.9.91 (9136)

F. Bancilhon, P. Lockemann, D. Tsichritzis (editors):
Directions of Future Database Research, Dagstuhl-Seminar-Report; 21, 9.9.-12.9.91 (9137)

H. Alt , B. Chazelle, E. Welzl (editors):
Computational Geometry, Dagstuhl-Seminar-Report; 22, 07.10.-11.10.91 (9141)

F.J. Brandenburg , J. Berstel, D. Wotschke (editors):
Trends and Applications in Formal Language Theory, Dagstuhl-Seminar-Report; 23, 14.10.-18.10.91 (9142)

H. Comon , H. Ganzinger, C. Kirchner, H. Kirchner, J.-L. Lassez , G. Smolka (editors):
Theorem Proving and Logic Programming with Constraints, Dagstuhl-Seminar-Report; 24, 21.10.-25.10.91 (9143)

H. Noltemeier, T. Ottmann, D. Wood (editors):
Data Structures, Dagstuhl-Seminar-Report; 25, 4.11.-8.11.91 (9145)

A. Dress, M. Karpinski, M. Singer(editors):
Efficient Interpolation Algorithms, Dagstuhl-Seminar-Report; 26, 2.-6.12.91 (9149)

B. Buchberger, J. Davenport, F. Schwarz (editors):
Algorithms of Computeralgebra, Dagstuhl-Seminar-Report; 27, 16.-20.12.91 (9151)

K. Compton, J.E. Pin , W. Thomas (editors):
Automata Theory: Infinite Computations, Dagstuhl-Seminar-Report; 28, 6.-10.1.92 (9202)

H. Langmaack, E. Neuhold, M. Paul (editors):
Software Construction - Foundation and Application, Dagstuhl-Seminar-Report; 29, 13..-17.1.92 (9203)

K. Ambos-Spies, S. Homer, U. Schöning (editors):
Structure and Complexity Theory, Dagstuhl-Seminar-Report; 30, 3.-7.02.92 (9206)

B. Booß, W. Coy, J.-M. Pflüger (editors):
Limits of Modelling with Programmed Machines, Dagstuhl-Seminar-Report; 31, 10.-14.2.92 (9207)

K. Compton, J.E. Pin , W. Thomas (editors):
Automata Theory: Infinite Computations, Dagstuhl-Seminar-Report; 28, 6.-10.1.92 (9202)

H. Langmaack, E. Neuhold, M. Paul (editors):
Software Construction - Foundation and Application, Dagstuhl-Seminar-Report; 29, 13.-17.1.92 (9203)

K. Ambos-Spies, S. Homer, U. Schöning (editors):
Structure and Complexity Theory, Dagstuhl-Seminar-Report; 30, 3.-7.2.92 (9206)

B. Booß, W. Coy, J.-M. Pflüger (editors):
Limits of Information-technological Models, Dagstuhl-Seminar-Report; 31, 10.-14.2.92 (9207)

N. Habermann, W.F. Tichy (editors):
Future Directions in Software Engineering, Dagstuhl-Seminar-Report; 32; 17.2.-21.2.92 (9208)

R. Cole, E.W. Mayr, F. Meyer auf der Heide (editors):
Parallel and Distributed Algorithms; Dagstuhl-Seminar-Report; 33; 2.3.-6.3.92 (9210)

P. Klint, T. Reps, G. Snelting (editors):
Programming Environments; Dagstuhl-Seminar-Report; 34; 9.3.-13.3.92 (9211)

H.-D. Ehrich, J.A. Goguen, A. Sernadas (editors):
Foundations of Information Systems Specification and Design; Dagstuhl-Seminar-Report; 35; 16.3.-19.3.9 (9212)

W. Damm, Ch. Hankin, J. Hughes (editors):
Functional Languages:
Compiler Technology and Parallelism; Dagstuhl-Seminar-Report; 36; 23.3.-27.3.92 (9213)

Th. Beth, W. Diffie, G.J. Simmons (editors):
System Security; Dagstuhl-Seminar-Report; 37; 30.3.-3.4.92 (9214)

C.A. Ellis, M. Jarke (editors):
Distributed Cooperation in Integrated Information Systems; Dagstuhl-Seminar-Report; 38; 5.4.-9.4.92 (9215)

J. Buchmann, H. Niederreiter, A.M. Odlyzko, H.G. Zimmer (editors):
Algorithms and Number Theory, Dagstuhl-Seminar-Report; 39; 22.06.-26.06.92 (9226)

E. Börger, Y. Gurevich, H. Kleine-Büning, M.M. Richter (editors):
Computer Science Logic, Dagstuhl-Seminar-Report; 40; 13.07.-17.07.92 (9229)

J. von zur Gathen, M. Karpinski, D. Kozen (editors):
Algebraic Complexity and Parallelism, Dagstuhi-Seminar-Report; 41; 20.07.-24.07.92 (9230)

F. Baader, J. Siekmann, W. Snyder (editors):
6th International Workshop on Unification, Dagstuhl-Seminar-Report; 42; 29.07.-31.07.92 (9231)

J.W. Davenport, F. Krückeberg, R.E. Moore, S. Rump (editors):
Symbolic, algebraic and validated numerical Computation, Dagstuhl-Seminar-Report; 43; 03.08.-07.08.92 (9232)

R. Cohen, W. Wahlster (editors):
3rd International Workshop on User Modeling, Dagstuhl-Seminar-Report; 44; 10.-14.8.92 (9233)

R. Reischuk, D. Uhlig (editors):
Complexity and Realization of Boolean Functions, Dagstuhl-Seminar-Report; 45; 24.08.-28.08.92 (9235)

Th. Lengauer, D. Schomburg, M.S. Waterman (editors):
Molecular Bioinformatics, Dagstuhl-Seminar-Report; 46; 07.09.-11.09.92 (9237)

V.R. Basili, H.D. Rombach, R.W. Selby (editors):
Experimental Software Engineering Issues, Dagstuhl-Seminar-Report; 47; 14.-18.09.92 (9238)

Y. Dittrich, H. Hastedt, P. Schefe (editors):
Computer Science and Philosophy, Dagstuhl-Seminar-Report; 48; 21.09.-25.09.92 (9239)

R.P. Daley, U. Furbach, K.P. Jantke (editors):
Analogical and Inductive Inference 1992 , Dagstuhl-Seminar-Report; 49; 05.10.-09.10.92 (9241)

E. Novak, St. Smale, J.F. Traub (editors):
Algorithms and Complexity of Continuous Problems, Dagstuhl-Seminar-Report; 50; 12.10.-16.10.92 (9242)

J. Encarnação, J. Foley (editors):
Multimedia - System Architectures and Applications, Dagstuhl-Seminar-Report; 51; 02.11.-06.11.92 (9245)

F.J. Rammig, J. Staunstrup, G. Zimmermann (editors):
Self-Timed Design, Dagstuhl-Seminar-Report; 52; 30.11.-04.12.92 (9249)