# Algorithmen und Zahlentheorie

26.10 - 30.10.98

organized by

Harald Niederreiter, Michael E. Pohst, Andrew Odlyzko

This seminar was the third one on number theoretical algorithms at Dagstuhl over the past 7 years. A major goal was always to bring together number theorists who develop the theory for efficient algorithms and people writing the corresponding software for applications. This year we had 42 participants from 13 countries.
In the last few years number theoretical applications to Coding Theory and Cryptography have become more and more important. Hence, it was no surprise that the majority of talks was on topics related to these applications. We would like to mention:

- computations with elliptic curves over finite fields; several new and efficient methods were presented; elliptic curve methods are currently under consideration for becoming part of the new standard for public key cryptosystems;
- primality testing and proving, large primes being of importance for quite a few cryptosystems;
- finite field algorithms, factorization of polynomials over finite fields; the ability to do efficient computations in and with finite fields is a basis for almost all algorithms applied in practice in the areas mentioned; factoring methods for polynomials over finite fields were tremendously improved over the last years;
- class group computations in global fields; since the usefulness of class groups of quadratic number fields for cryptographical applications was demonstrated, this has become a new area of research on a class of basic objects from pure mathematics; as for now the constructive approach is still limited to global fields of small degree.

In the other talks given a large variety of problems in algorithmic (algebraic) number theory was treated as the reader will notice from the subsequent abstracts.
For the organizers it was not easy to squeeze the large number of talks into one week's schedule. Fortunately, most of the talks were short, so that there was still ample time for stimulating discussions. Of course, the special atmosphere of Schloß Dagstuhl also contributed to a very productive meeting.

# Contents

# 1 Arithmetic of modular curves and applications

Gerhard Frey, Institute for Experimental Mathematics, University of Essen, Germany

The lecture gave a report on algorithms used to determine the space of cusp forms with respect to the congruence subgroups $\Gamma_0(N)$ as Hecke-ring module with Galois action. The relation with geometric-arithmetic objects like modular curves $X_0(N)$, their Jacobians $J_0(N)$ and corresponding $L-$series was explained.
The main algorithm uses Manin's theory of modular symbols. It can be used to determine simple factors of $J_0(N)$ and to compute Fourier expansions of cusp forms. Applications to modular elliptic curves are the computation of the modular degree which is closely related to the $ABC-$conjecture and the finding of elliptic curves with Galois-isomorphic torsion structures.
The period matrix of $J_0(N)$ resp. of its factors can be computed with high precision and so (using results of Weber, Mumford, Poor and Mestre) the equation of hyperelliptic curves defined over $Q$ with real multiplication can be determined.
Finally we presented results of Ch. Hahne who used Arakelov intersection theory to compute the Néron-Tate height on the Jacobian of these hyperelliptic curves and, by using the conditional algorithm of Manin, is able to compute a base of their Mordell-Weil group .
(For more details cf. G.Frey, M. Müller: Arithmetic of modular Curves and applications, preprint No. 20 (1998) IEM.,Essen.)

# 2 Primality proving and modular curves

Francois Morain, LIX - Palaiseau Ecole Polytechnique, France

One of the problems encoutnered in implementing the Elliptic Curve Primality Proving algorithm is that of building the reduction of an elliptic curve $E$ defined over the Hilbert Class Field $K_H$ of the imaginary quadratic field $Q(\sqrt{-D})$, $D > 0$. More precisely, if $p$ is a rational prime that splits in $K_H$ (which is equivalent to $4p = U^2 + DV^2$ in rational integers $U$ and $V$), there exists a curve $E/F_p$ such that $\#E = p + 1 - U$. There is a sign ambiguity on $U$, that can be solved using

a variety of methods: Here we show how to solve the problem when $3|D$, using the class invariant $(\eta(z/3)/\eta(z))^{12}$ which is connected to $X_0(3)$. Similar resulsts on class invariants are also given for each $N$ for which $X_0(N)$ has genus 0.

# 3 On $\Sigma\bowtie$-representations of integers

Attila Pethő, Debrecen, Hungary

The talk is based on a joint paper with J. Demetrovics and L. Rónyai, which is submitted for publication to Acta Cybernetica.
Let $n$ be a non-zero integer. The representations

$$n = \sum_{i=0}^{l'} d_i 2^i, \quad d_i = -1, 0, 1;\ i = 1, \ldots, l';\ d_{l'} = 1,$$

are called $\pm 1$-representation of $n$. This representation is not at all unique. Consider for example $n = (1100)^k 1$. Then replacing $\ell$ $(0 \leq \ell \leq k)$ blocks of form 1100 with the block $(-1)010$ we obtain $2^k$ different $\pm 1$-representations of the same length of $n$.
We call a $\pm 1$-representation *optimal*, if $l' + \sum_{i=0}^{l'} |d_i|$ is minimal among the $\pm 1$-representations of $n$. The aim of our talk was to prove the following theorem:

**Theorem** *There exists an algorithm which computes an optimal $\pm 1$-representation of the integer $n$ in $O(\log |n|)$ additions and comparisons.*

In order to prove our theorem we associate to the integer $n$ an infinite, bipartite, directed, acyclic graph $G(n)$ such that the $\pm 1$-representations of $n$ correspond to suitable directed paths in $G(n)$. Next we establish that to find an optimal $\pm 1$-representation it suffices to consider a subgraph of $G(n)$ having at most $2 \log_2 n + 5$ nodes. Our problem is actually equivalent to a single source shortest paths problem in this graph, which can be solved fast using a variant of the well known Dijkstra algorithm.

# 4 Computation of Galois groups

Katharina Geißler, TU-Berlin, Germany

We present an extended version of the method of Stauduhar, which in particular allows us to compute more efficiently Galois groups of higher degrees, e.g. Galois groups of univariate polynomials $f$ over the rationals up to degree 15. This algorithm combines the relative resolvent method with the computation of subfields of algebraic number fields $Q(\alpha)$, with $f(\alpha) = 0$. The extension of Stauduhar's method can be realized for imprimitive transitive permutation groups:

(i) By Krasner's and Kaloujnine's theorem a transitive imprimitive permutation group with a block system, which consists of $m$ blocks of length $l$, can be embedded in a wreath product of the form $S_l \wr S_m$. We arrive at this information in the algorithm by computing subfields $Q(\alpha)$ of degree $m$, which are in bijection with the blocks $B$ of length $l$ of $Gal(f, Q)$ which contain $\alpha$.

(ii) Let $g$ be the minimal polynomial generating a subfield of $Q(\alpha)$ of degree $m$. The operation of $Gal(f, Q)$ on the Blocks $B$ of length $l$ which contain $\alpha$ is equivalent to the operation of $Gal(g, Q)$ on the roots of $g$.

That means $Gal(f, Q) \leq S_l \wr Gal(g, Q) \leq S_l \wr S_m$.

With this additional information we can change the starting point in Stauduhar's algorithm to get as close as possible to the actual Galois group. This tends to be very time saving, because we can always skip the first step (or even all steps) of the algorithm. Moreover we describe our implementation and give some experimental results for irreducible polynomials of degree 14 and 15.

# 5 Constructive Classfield Theory

Claus Fieker, TU-Berlin, Germany

Essentially based on the proof of the existence theorem of Class Field theory (e.g. as in Serge Lang's Number Theory) and using explicit versions of the Artin map, we demonstrate how to compute (defining equations for) Class Fields.
More precisely: Given $k/Q$ a numberfield, a module $m$ and an ideal group $P_m \leq H \leq H^m$ we will compute $K/k$ s.t. $\mathrm{Gal}(K/k) \equiv I^m/H$. This is done in two steps: First, construct $E = k(\zeta)$ with a suitable root of unity $\zeta$. Then, using Kummer theory and S-units, build a large field $G$ known to contain $F$ the Class Field corresponding to $N_{E/k}^{-1}(H)E^*$. Using explicit representations for $\mathrm{Gal}(G/E)$ and the Artin map $a \mapsto (a, G/E)$ we obtain a Kummer generator for $F/E$.

In a second step we start by computing $\mathrm{Gal}(F/k)$. Since this is an abelian group, we can again use the Artin map to find $\mathrm{Fix}(K) \leq \mathrm{Gal}(F/k)$, the group fixing $K$. Using elementary Galois theory it is now an easy task to construct a primitive element $\beta$ for $K/k$.

# 6 The Class Numer One Problem for some Non-Abelian Normal CM-Fields

Michel Olivier, Universite Bordeaux I, France

Joint work with S. Louboutin and R. Okazaki.
After the work of K. Uchida, H. M. Stark, A. M. Odlyzko, J. Hoffstein and al. we know that there exist only finitely many normal CM-fields with class number one. K. Yamamura (1994) have computed all the imaginary abelian number fields with class number one.
In the first part of the talk, we give a survey of the known results for the class number one problem for the non-abelian normal CM-fields. This problem is now solved for degree 8, 12, 16, 20 (partial result), 24 (partial result) (the only possible degrees up to 26).
In the second part, we deal as an example with the degree 12 case. We prove that there are exactly 16 non-abelian normal CM-fields of degree 12 with relative class number one (all are dihedral) ; exactly 9 out of them have class number one.
For details, see Trans. Am. Soc., 349, 1997, p. 3657–3678.

# 7 Power Integral Bases in Algebraic Number Fields

Istvàn Gaàl, Debrecen, Hungary

Let $K$ be an algebraic number field of degree $n$ with ring of integers $\mathbb{Z}_K$. It is a classical problem in algebraic number theory to decide if $K$ admits a **power integer basis**, that is an integer basis of the form $\{1, \alpha, \ldots, \alpha^{n-1}\}$.

If $\{1, \omega_2, \ldots, \omega_n\}$ is any integer basis of $K$, then $D_{K/Q}(X_2\omega_2 + \ldots + X_n\omega_n) = (I(X_2, \ldots, X_n))^2 D_K$ where $I(X_2, \ldots, X_n)$ is the **index form** corresponding to the above integer basis and $D_K$ is the discriminant of $K$. The element $\alpha = x_1 + \omega_2 x_2 + \ldots + \omega_n x_n \in \mathbb{Z}_K$ generates a power integral basis if and only if

$$I(x_2, \ldots, x_n) = \pm 1.$$

Hence the problem of determining power integral bases can be reduced to the resolution of the above **index form equation**.
The talks gives a survey of the algorithms for solving index form equations in different types of number fields, including also some recent developments.
There are efficient algorithms for lower degree number fields (cubic, quartic). Using the enumeration method of Wildanger it became now possible to solve index form equations in any quintic fields (I.Gaál and K.Győry, 1998).
In the case of sextic fields, the problem is solved for fields with a quadratic subfield (I.Gaál and M.Pohst 1997).
Recently we succeded to solve index form equations in octic fields with a quadratic subfield (I.Gaál and M.Pohst 1998). In this case an essential role was played by a new algorithm for solving relative Thue equations (I.Gaál and M.Pohst 1998) based also on Wildanger's method.
We also obtained results for some higher degree fields which are composits of subfields, for example for fields of degree nine with cubic subfields (I.Gaál 1998).

# 8 Efficient elliptic curve exponentiation

Henri Cohen, Universite Bordeaux I, France

joint work together with A. Miyaji and T. Ono

We give several new ideas for improving the efficiency of elliptic curve exponentiation $Q \leftarrow N \cdot P$ over a large prime field.
• The use of modified Jacobian coordinates $(x, y, z, az^4)$ where the affine equation of the curve is $y^2 = x^3 + ax + b$ and the point is $(x/z^2, y/z^3)$. This is the fastest possible method for doubling on the curve.
• The use of a mixed coordinate strategy: use modified Jacobian for repeated doublings (most of the time), but use Jacobian mixed with affine for additions (fastest possible), with initial precomputed points in affine coordinates.
• The use of Montgomery's trick for the precomputed points in affine coordinates. For example to compute $P$, $3P$, $5P$,...,$15P$ we compute in parallel using Mongomery's trick $2P$, $(3P, 4P)$, $(5P, 7P, 8P)$, $(9P, 11P, 13P, 15P)$.

• The use of special techniques for the initial Horner evaluation. For example, instead of computing $64P$ in 6 doublings, we compute $4(15P + P)$ using 2 doublings and one addition. This is efficient because the analysis shows that the initial digit in Horner's scheme is equal to 1 or to a small digit with high probability.
• We give a detailed analysis of the flexible window method. If the width is $e$ bits and $N$ has $n$ bits, the average number of doublings is $n - e(e-1)/(2(e+1))$, the average number of addition/subtractions is $n/(e+1) - (e-1)(e+2)/(2(e+1)^2)$ (in addition to the initial computations which are done differently), and the average gain obtained from the clever initial Horner evaluation is $(e^2 + 3e - 6)/(2e + 2)$ doublings minus $e/(e + 1)$ addition/subtractions.
All together, on a cryptographic range application ($n = 256$, $e = 5$, 256 bit prime field) the gain is around 20%.

# 9 On some recent computations

Franz Lemmermeyer, Universitat des Saarlandes, Germany

1. In order to make the well known connection between Selmer groups of elliptic curves and 2-class groups of cubic number fields more explicit, we started studying connections between the rank of the elliptic curve and the 2-rank of cubic number fields. Combining proofs of Billing and Cassels, we can show that the ranks $r_k$ of $E_k : y^2 = x^3 - k$, $k \not\equiv \pm 1 \bmod 9$ cubefree and odd, satisfy the inequality $r_k + r_{-k} \le 2R + 1$, where $R$ denotes the rank of the 2-class group of $Q(\sqrt[3]{k}\,)$.
2. We reported on progress concerning the classification of complex quadratic number fields whose 2-class fields have 2-class groups of rank 2.
3. Finally we presented results on the computation of totally real cubic fields that are norm-Euclidean (in the range $0 < \operatorname{disc} K < 13,000$) or Euclidean with respect to some weighted norm (with $0 < \operatorname{disc} K < 8,000$).

# 10 Isomorphisms between Artin-Schreier Towers

Jean-Marc Couveignes, Université de Toulouse II, France

Let $\mathbf{F}_q$ be a finite field with $q = p^d$ elements. Let $L_n$ be an extension of degree $p^n$ of $\mathbf{F}_q$, given as a tower

$$L_n \supset L_{n-1} \supset ... \supset L_1 \supset L_0 = \mathbf{F}_q \quad (1)$$

of non-trivial Artin-Schreier extensions each defined by

$$L_{k+1} = L_k(x_{k+1}) \text{ with } x_{k+1}^p - x_{k+1} - a_k = 0 \text{ and } a_k \in L_k.$$

Artin-Schreier towers naturally arise in computational algebraic geometry. In particular, let $G = Gal(\bar{\mathbf{F}}_q/\mathbf{F}_q)$ be the absolute Galois group of $\mathbf{F}_q$. Morphisms between abelian varieties $A$ and $B$ defined over $\mathbf{F}_q$ induce $G$-morphisms between the Tate modules $\mathcal{T}_p(A)$ and $\mathcal{T}_p(B)$. Assume the $p$-torsion of $A$ and $B$ is defined over $\mathbf{F}_q$. One can easily show that the definition field $L_k$ of the $p^{k+1}$-torsion of $A$ is an extension of $L_0 = \mathbf{F}_q$ with degree dividing $p^k$. Similarly the definition field $M_k$ of the $p^{k+1}$-torsion of $B$ is an extension of $M_0 = L_0 = \mathbf{F}_q$ with degree dividing $p^k$.

Assuming the existence of an isogeny between $A$ and $B$ with prime to $p$ degree, the fields $L_k$ and $M_k$ are isomorphic. These fields can be constructed by taking successive preimages of a $p$-torsion point by separable isogenies of degree $p$. Thus they naturally come as Artin-Schreier towers. In the case of non-supersingular elliptic curves, such isogenies are described in terms of Hasse functions. If we are looking for an isogeny with a given prime to $p$ degree between $A$ and $B$, we can compute it by interpolation at enough $p^k$-torsion points. This reduces to computing an isomorphism between the Artin-Schreier towers we have on each side. This method is of special interest for computing the cardinality of ordinary elliptic curves with the Schoof-Elkies-Atkin algorithm. In a previous work, the fastest known algorithm for this purpose is given, assuming the characteristic $p$ is fixed.

We prove that an isomorphism between two Artin-Schreier towers of degree $p^n$ can be computed in time essentially linear in $p^n$.

Our algorithm relies on an iterative approximation process with respect to the following "distance". If $\alpha, \beta \in L_n$ we define the *écart* $\mathbf{d}(\alpha, \beta)$ to be the logarithm (with base $p$) of the degree of the extension $\mathbf{F}_q(\alpha - \beta)/\mathbf{F}_q$. The triangle inequality is easily checked. Note that $\mathbf{d}$ is not a distance since $\mathbf{d}(\alpha, \beta) = 0$ if and only if $\alpha - \beta$ is in $\mathbf{F}_q$.

# 11 Elliptic Curves and Discrete Logarithms

Hans-Georg Rück, Institut fur Experimentelle Mathematik, Universität GH Essen, Germany

joint work together with G. Frey and M. Müller

In each group $G$ the "exponentiation" $Q = n \cdot P$ ($n \in N, P \in G$) can be performed in $O(\log n)$ steps. Groups are useful for cryptographic reasons, if the inverse operation, the "discrete logarithm" $n = \log_P Q$ ($P, Q \in G$), is not a polynomial time or subexponential time algorithm.
In this talk we considered the group $G = E(F_q)_m$, the $m$-torsion group of $F_q$-rational points on an elliptic curve $E$ over the finite field $F_q$. We explained that the discrete logarithm in $E(F_q)_m$ can be reduced in $O(\log m)$ steps to the discrete logarithm in $F_q^*$ or $F_q$ (which can be solved in subexponential or polynomial time) by the Tate pairing in the cases that $q \equiv 1 \bmod m$ or $m = \mathrm{char}(F_q)$. Hence these two cases should be avoided at the design of a cryptosystem.

# 12 A Sequentiell Implementation of the Black-Box Niederreiter Algorithm for Factoring Polynomials over the Binary Field

Markus Holder, Institut für Experimentelle Mathematik, Universität GH Essen, Germany

joint work together with P. Fleischmann, Peter Roelse

We describe an implementation of Niederreiter's polynomial factorization algorithm using Wiedemann's method to solve linear equations.
The requirement for the application of Wiedemann's method is a fast performance of the product matrix · vector. For the Niederreiter matrix this can be accomplished using fast polynomial arithmetic.
The main advantage of the algorithm is the low memory requirement (only $O(n)$). Therefore with our sequentiell implementation we are able to factor high degree polynomials over $F_2$ on a single workstation. Of course, this implementation doesn't beat existing parallel implementations as for instance the one of Peter Roelse.
An important future direction will be the parallelization of the algorithm using Block–Wiedemann or Block–Lanczos ideas.

# 13 Average–case Analyses of a class of Euclidean algorithms. Dynamical mehods and functional analysis

Brigitte Vallée, Université de Caen, France

We provide here a complete average–case analysis of seven Euclidean algorithms; some of thencan be used for computing the Jacobi symbol. We analyse the average number of steps used for each ofthe algorithms on integers less than $N$. We exhibit two different kinds of behaviour: some of these algorithms are "fast", and the average number of steps is shown to be asymptotic to $A \log N$, whereas others algorithms are "slow", and the average number of steps is shown to be asymptotic to $B \log^2 N$.
Some of these results are well–known, whereas the analysis of the Binary GCD [Vallée98] or the analyses of three algorithms for the Jacobi symbol [Vallée, Lemée98] are new. However, we present a general method which unifies all the analyses. This method uses quite varied tools: generating functions, Ruelle operators , Tauberian methods, functional analysis. First, we use classical tools in the average–case analysis of algorithms: we introduce the generating functions related to the parameters to be analyzed; as is usual in the context of computational number theory, these generating functions are Dirichlet series. Second, we prove that these generating functions are closely linked to some operators associated to the algorithms. These operators contain all the information on the dynamics of the algorithm. In the context of dynamical systems, they are called the Ruelle operators relative to the system. More precisely, the generating functions involve the quasi–inverse operator $(I - \mathbf{H}_s)^{-1}$, and the expectations to be studied are partial sums of coefficients of these Dirichlet series, so the main results of the paper will come from the application of Tauberian Theorems, provided that they *can* be applied. This will be the case as soon as the operator $\mathbf{H}_s$ when acting in a suitable Banach space has a "spectral gap", i.e., a unique dominant eigenvalue separated from the remainder of the spectrum by a gap. When acting on suitable spaces of holomorphic functions, the operator $\mathbf{H}_s$ is proven to be compact and positive (in the sense of Krasnoselsky) for real values of parameter $s$, and then it has a spectral gap. Since Tauberian theorems link the asymptotics of coefficients to the dominant singularity of the function, the constants $A_i$ involve the dominant singularity of the quasi–inverse $(I - \mathbf{H}_s)^{-1}$, i.e. the dominant spectral objects of the Ruelle operator $\mathbf{H}_s$. These dominant spectral objects are explicit in some cases, but, for other algorithms, they do not seem be related to other classical constants.

# 14 An LLL algorithm for totally positive lattices over number fields

Alexander Schiemann, Universität des Saarlandes, Germany

Let $F$ be a totally real number field, $E$ a quadratic extension and $V$ an $n$-dimensional $E$-space with totally positive hermitian form $h$, i.e. $T := tr_{E/Q} \circ h$ is positive definite. An $\mathcal{O}_E$-lattice $L$ in $V$ has a representation $L = \sum_{l=1}^{n} a_l x_l$ with fractional ideals $a_i$ which is called a pseudo-base. Starting with such a base we want to find another one with small $T(x_i, x_i)$ and ideals that are reduced in some sense. It turns out that the conditions given below can be matched by an algorithm very similar to the LLL for $Z$-lattices and that they imply similar bounds for the quality of the result. This is an advantage compared to LLL-versions suggested by Fieker in a more general context.
For $L = \sum_{l=1}^{n} a_l x_l$ let $p_i$ denote the orthogonal projection on $(\sum_{l=1}^{i-1} E x_l)^{\perp}$, $x_i^* := p_i(x_i)$. Let $L_{ij} := \sum_{l=i}^{j} a_l x_l$ and for a discrete set $L'$ let $\mu_T(L') := \min\{T(x,x) \mid x \in L' \setminus \{0\}\}$.
The pseudo-base is called $(k, q, q_1)$-reduced (for constants $q, q_1$ subject to $0 < q < 1$, $0 < q_1 \leq 1$ and "blocksize" $k \in \{2, \ldots, n\}$) iff

1. $\forall\, i = 1, \ldots, n : \quad a_i \supseteq \mathcal{O}_E$
2. $\forall\, i = 1, \ldots, n$ with $b(i) := \min(n, i + k - 1)$ :
$$q\, T(x_i^*, x_i^*) \leq \mu_T(p_i(L_{i,b(i)}))$$
3. $\forall\, 1 \leq j < i \leq n$ :
$$q_1\, T(p_j(x_i)\,,\, p_j(x_i)) \leq \mu_T\Big(p_j(\{x_i + \alpha x_j \mid \alpha \in a_i^{-1} a_j\})\Big).$$

By translating everything back to $Z$-lattices we can prove:

- $\mathrm{N}_{E/Q}(a_i^{-1}) \leq \left(\frac{\gamma_m}{qm}\right)^{m/2} |\,\mathrm{d}_E|^{1/2}$,
where $m = [E : Q]$ and $\gamma_m$ is Hermite's constant.
- $T(x_i^*, x_i^*) \leq C_1\, T(x_{i+1}^*, x_{i+1}^*)$ with $C_1 = \left(\frac{\gamma_{2m}}{qm}\right)^2 |\,\mathrm{d}_E|^{2/m}$.
- $T(x_1, x_1) \leq q^{-1}\, C_1^{n-1}\, \mu_T(L)$.
- There is a positive constant $C_2(i)$ not depending on $L$ or $T$ such that $T(x_i, x_i) \leq C_2(i)\, T(x_i^*, x_i^*)$.

An implementation of this algorithm for complex quadratic fields showed much better results than any other method we tried.

# 15 Numerical verification of the conjecture of Ankeny, Artin, and Chowla for the primes $< \bowtie\mho^{11}$

Herman te Riele, CWI Amsterdam, Netherlands

joint work together with Hugh Williams

Let $p \equiv 1 \bmod 4$ be a prime. The Ankeny-Artin-Chowla (AAC) Conjecture asserts that if the fundamental unit $\epsilon$ of $Q(\sqrt{p}\,)$ is given by $(x + y\sqrt{p}\,)/2$, then $p \nmid y$.
If $k \in N$ is such that $(p, k) = 1$ and if $\epsilon^k = (X + Y\sqrt{p}\,)/2, \quad X, Y \in Z$, then $p|Y \Leftrightarrow p|y$. Our strategy is to estimate a value $\log_2 \epsilon^h$ where $h$ is the class number of $Q(\sqrt{p}\,)$ and use this to determine a value $\eta \in Z$ (defined in the paper) which has the property that $p|\eta \Leftrightarrow p|Y$. For this estimate, we make use of the analytic class number formula: $2h \log \epsilon = \sqrt{p} L(1, \chi_p)$; let $R := \log_2 \epsilon$.

*Global algorithm*
1. Find an estimate of $hR$ by estimating $L(1, \chi_p)$;
2. from this, find the value of $hR$ which is accurate to within machine accuracy, by using Shanks' baby-giant step algorithm, and check that $hR < 8p$ (which ensures that $\gcd(p, h) = 1$);
3. compute $\eta = \eta(hR)$ and verify $\eta(hR) \not\equiv 0 \bmod p$.

So far, the AAC conjecture was verified for all the primes $\equiv 1 \bmod 4$ less than $10^9$ by Stephens and Williams (Math. Comp. **50**(1988)619–632). We have confirmed now the truth of the AAC conjecture for all the primes $\equiv 1 \bmod 4$ between $10^9$ and $10^{11}$. The above algorithm was implemented in Fortran 77 and tested and run on a workstation supporting 64-bit arithmetic, which was very helpful in view of the size of the primes for which we wanted to verify the AAC conjecture. Computing times were 250 and 700 CPU hours on an SGI O2 workstation and on one processor of an SGI Origin 2000, respectively, for intervals of primes of length $8 \times 10^9$ and $91 \times 10^9$, respectively.

# 16 Zeroes of Eisenstein series

Ernst-Ulrich Gekeler, Universität des Saarlandes, Saarbrücken, Germany

Let $E_k(z) = \text{const.} \sum_{a,b \in Z} \frac{1}{(az+b)^k}$ ($k \geq 4$ even) be the Eisenstein series of weight $k$, normalized such that its Fourier expansion has constant term 1: $E_k = 1 + \sum_{n \geq 1} a_n q^n$.
Then the $a_n$ are rational, and $E_k$ can be calculated as $E_k = A_k(E_4, E_6)$ with some isobaric polynomial $A_k \in Q[X,Y]$ of weight $k$. $A_k$ may be determined through a complicated recursion that comes from the functional equation of Weierstraß $\wp$-functions.
Fix a prime $p \geq 5$ and put

$$\varphi_p(X) = \Pi(X - j) \in Q[X],$$

where $j$ runs through the $j$-values $\neq 0, 1728$ of zeroes of $E_{p-1}$. It is known (Rankin, Swinnerton-Dyer) that these are real and satisfy $0 < j < 1728$. The polynomial $\varphi_p$ is a one-variable dehomogenized version of $A_{p-1}(X,Y)$, deprived from its "trivial" zeroes. It has $p$-integral coefficients, and

$$\tilde{\varphi}(X) = \prod_{\substack{j \in \overline{F}_p \\ j \text{ supersingular}, \neq 0,1728}} \in F_p[X],$$

denoting reduction (mod $p$) by ( $\tilde{}$ ). Hence the $j$-zeroes of $E_{p-1}$ provide "canonical" lifts of supersingular invariants to characteristic zero.
Based on numerical evidence for small primes $p$ ($p \leq 107$) and from the analogous function field setting (where a part of the following may be proved: joint work with G. Cornelissen), we conjecture:

(i) $\varphi_p$ is always irreducible

(ii) the Galois group of $\varphi_p$ is always the full symmetric group.

We further observe a very strong divisibility pattern of the discriminant $\text{disc}(\varphi_p)$ by the primes $l \leq \frac{p-1}{2}$, for which we presently have no explanation.

# 17 The Mordell-Weil group of elliptic curves over number fields

Susanne Schmitt, Universität Saarbrücken, Germany

The Mordell-Weil group of an elliptic curve over a number field forms a finitely generated abelian group. I described an algorithm with which in theory one can determine this group.
The computation of the torsion group is done by first estimating the number of torsion points and then computing the torsion points by means of division polynomials.
For computing the rank of elliptic curves, there are two methods: descent methods and the conjecture of Birch and Swinnerton-Dyer. These methods led to several implementations of algorithms for elliptic curves over the rational numbers. Up to now, there was only one general algorithm which determines the rank of elliptic curves over number fields. This was done by Pascale Serf. She implemented 2-descent for real quadratic number fields with class number one. Since it doesn't seem possible to extend her methods any further, my aim was to give an algorithm which is based on the conjecture of Birch and Swinnerton-Dyer. I developed a conditional algorithm which computes the rank of elliptic curves over number fields. If one assumes that one has enough time and space, this algorithm has no restriction on the number field.
For the computation of a basis of an elliptic curve over number fields, I first search for a subgroup of full rank. Then I use a theorem of S. Siksek to estimate the index of this group in the whole group. With this estimate, it is possible to compute a basis.
I am working on the implementation of this algorithm for elliptic curves over quadratic number fields in the computer algebra system SIMATH.

# 18 Bases of Cyclotomic Units

Marc Conrad, Universität Saarbrücken, Germany

For $n \in \mathbf{N}$ let $\epsilon_n = e^{\frac{2\pi i a}{n}}$ with $(a,n) = 1$ a primitive $n$-th root of unity and $D^{(n)}$ the multiplicative group generated by elements of the form $1 - \epsilon_n^k$ with $k \not\equiv 0 \bmod n$ modulo unit roots. The group of *cyclotomic units* is defined as $C^{(n)} = (\mathbf{Z}[\epsilon_n]^* / \langle \pm\epsilon_n \rangle) \cap D^{(n)}$. Our aim is to construct a basis of $C^{(n)}$.
Let $M$ be a free module with an involution $\sigma$ and $M_+ = M/\ker_M(1+\sigma)$. For an ordered indexing set $\Delta$ we introduce a system of triples $(M_d, \mathcal{E}_d, \mathtt{n}_d)_{d\in\Delta}$, where $M_d$ is a module, $\mathcal{E}_d \subseteq M_d$ and $\mathtt{n}_d : \mathcal{E}_d \to \bigoplus_{t<d} M_t$ is a mapping for each $d \in \Delta$. Such a system defines a module

$$\mathcal{L} = (\bigoplus_{d\in\Delta} M_d) / \sum_{d\in\Delta} \langle r + \mathtt{n}_d(r);\ r \in \mathcal{E}_d \rangle$$

which we call the *combination* of the system. We show how to construct a basis of $\mathcal{L}_+$ using special bases, the so called *weak $\sigma$-bases* of the modules $M_d/\langle\mathcal{E}_d\rangle$. For well chosen input parameters $\Delta$, $M_d$, $\mathcal{E}_d$ and $\mathfrak{n}_d$ we obtain as combination a module $\mathcal{L}(n)$ for which an isomorphism $\mathcal{L}(n)_+ \cong D^{(n)}$ holds. This leads to a basis for $D^{(n)}$ which can be easily modified to a basis for $C^{(n)}$. Moreover we obtain a basis $B_n$ for $C^{(n)}$ such that $B_d \subseteq B_n$ whenever $d|n$. This leads obviously to a basis of $\bigcup_{d\in\mathcal{N}} C^{(d)}$. Finally some other applications of these methods are discussed: The explicit construction of relations in $C^{(n)}$ and similar results for the Stickelberger ideal as for the group of cyclotomic units.

# 19 Numerical Construction of Class Fields by Elliptic Functions

Reinhard Scherz, Institut für Mathematik der Universität Augsburg, Germany

From complex multiplication we know that the Hilbert class field $H$ of an imaginary quadratic number field $K$ can be generated by the modular invariant $j(O)$ of its ring of integers $O$. However these generators are not very suitable for numerical purposes because the coefficients of their minimal polynomials are extremly high.

By Kronecker's limit formula it is suggested to consider units of the form

$$\epsilon(a) := \tfrac{\Delta(a)\Delta(a)}{\Delta(a^2)\Delta(O)},$$

where $\Delta$ denotes the discriminant from the theory of elliptic functions and $a$ an ideal of $O$. It has been shown that apart from trivial exceptions the Hilbert class field can always be generated by a 24-th root of a suitable number $\epsilon(a)$ and it turns out that their minimal polynomials have rather small coefficients.

A similar result is obtained for ray class fields using values of the type

$$\tfrac{\varphi(\xi|a^{-1})}{\varphi(\xi|O)}, \quad \xi \in K,$$

where $\varphi$ is a suitably normalized $\sigma$-function.

**Literatur**

Reinhard Schertz, Construction of Ray Class Fields by Elliptic Units, Journal de Théorie des Nombres de Bordeaux 9 (1977), 383-394.

Reinhard Schertz, Lower Powers of Elliptic Units, preprint.

# 20 Actual Computation of Units by the Cyclo-Elliptic Method (CEM)

Ken Nakamula, Tokyo Metropolitan University, Japan

Review of the CEM:
For the quadratic field of discriminant 229, we explain the process of computation by the CEM that the class number is 3 and the minimal polynomial of the fundamental unit is $X^2 - 15X - 1$.
Data by the CEM:
Existing printed tables by the CEM are listed. It is noticed that the table for quintic cyclic fields appeared only recently in 1998. We restarted a project to make an electronical database by the CEM, which will be put in

`ftp://ftp.math.metro-u.ac.jp/tnt/cem/*`

from now on. The cases done are computed by `PARI/GP`. The cases to be done are also announced.
Problems:

1. In `PARI/GP`, does the program, which computes the class group and the unit by McCurley's subexponential algorithm, applies to the case of non-fundamental discriminant?

2. We encountered to solove the diopantine equation $a^2 - b^2 d = n$ for a very small $d < -10^5$ and exceedingly large $n > 10^{100}$.

3. In the elliptic case, we should find out a good algorithm to determine the conductors of subgroups of a class group of an imaginary quadratic field. This task is theoretically possible, but still several technical problems should be solved.

4. Special investigation is necessary for each case to obtain sharp upper bounds of the unit indices occuring in the class number formula. In particular, we must study the case of cyclic quintic extensions of an imaginary quadratic field.

# 21 Efficient exponentiation in finite fields

Joachim von zur Gathen, Universität-GH Paderborn, Germany

Interest in the problem of the title comes from cryptography. Recent progress is based on choosing appropriate data structures for an extension of a finite field such as $F_2$.
The basic tool for one type of algorithms are **Gauß periods**. We show that one can combine this with fast polynomial arithmetic, and generalize these Gauß periods to extend their range of application.

# 22 Distribution of residues of exponential functions and algorithms

Igor Shparlinski, School of Mathematics, Physics, Computing and Electronics, Macquarie University, Australia

joint work together with Sergei Konyagin

In this talk we consider various questions related to the distribution of integer powers $g^x$ of some integer $g > 1$ modulo a prime number $p$ with $\gcd(g, p) = 1$. Possible algorithmic applications where such results play a central role include but are not limited to linear congruential pseudo-random number generators, algebraic number theory, finite fields, sorting algorithms, cryptography, and coding theory.

# 23 Divisors in Residue Classes, Constructively

Don Coppersmith, IBM Research, Yorktown Heights, NY, USA

joint work together with N. Howgrave-Graham

Let $r, s, n$ be integers satisfying $0 \le r < s < n$, $s \ge n^\alpha$, $\alpha > 1/4$, and $\gcd(r, s) = 1$. Hendrik Lenstra showed that the number of integer divisors of $n$ equivalent to $r \pmod{s}$ is upper bounded by $O((\alpha - 1/4)^{-2})$. We show how to construct all such divisors in polynomial time, and incidentally we improve the bound to

$O((\alpha - 1/4)^{-3/2})$. We do this by formulating a related polynomial problem, linearizing, and using lattice basis reduction techniques.

## 24 Efficient Computation of Minimal Polynomials of Extensions of Finite Fields

Victor Shoup, IBM Research Laboratory, Ruschlikon, Switzerland

New algorithms are presented for computing the minimal polynomial over a finite field $K$ of a given element in an algebraic extension of $K$ of the form $K[\alpha]$ or $K[\alpha][\beta]$. The new algorithms are explicit and can be implemented rather easily in terms of polynomial multiplication, and are much more efficient than other algorithms in the literature.

## 25 New Permutation Polynomials and Applications

Hans Dobbertin, BSI Bonn, Germany

We present a new systematic technique to prove that certain polynomials over GF(2) are permutation polynomials (pp's) on GF($2^n$). This method requires extensive algebraic computations, which can only be made with the help of computer algebra. A key step is the factorization of multivariate polynomials over GF(2). In this way we find new pp's and new proof for known pp's. Two classes of these new pp's are important ingredients to confirm long-standing conjectures of Welch and Niho on exponential sums. There are also various applications on correlation properties of sequences and on difference sets.

# 26 On some elliptic surfaces and elliptic curves related to discriminants of cubic or quartic polynomials

Franck, Leprévost, Université Paris 7, France and Technische Universität Berlin, Germany

On some elliptic surfaces and elliptic curves related to discriminants of cubic or quartic polynomials
We associate to each discriminant $t \neq 0$ of a polynomial of degree $n \geq 1$ an elliptic curve $E_t$. For each polynomial of degree $n = 3, 4$, we construct a rational point on $E_t(Q)$ which is generically non torsion. For $n = 4$, we prove that $E_t \simeq C$, where $C$ is the cubic associated by Gaàl, Pethö and Pohst to each quartic field. They also constructed a surface $S$ connected to the cubic $C$. We compute the Kodaira dimension and the dimension of the Albanese variety of $S$ and specify the class to which $S$ belongs in the classification of algebraic surfaces. We also answer a question of Pethö, and give statistical results, which were obtained in a joined work with S. Fermigier and C. Fieker.

These results are the subject of the following articles to appear in the *Journal of Number Theory*:

Sur certaines surfaces elliptiques et courbes elliptiques de Mordell de rang non-nul associées à des discriminants de polynomes cubiques ou quartiques.
F. Leprévost.

Appendice : quelques données statistiques.
S. Fermigier, F. Leprévost, Claus Fieker.

# 27 Ten Topics in computational number theory

Dan J. Bernstein, The University of Illinois at Chicago, USA

1. Fast Fourier Transforms
2. Dividing power series

3. Exponentiating power series
4. Enumerating primes
5. Bounding smooth integers
6. Smooth polynomial values
7. Square products
8. Pomerance's conjecture
9. Estimating transition time
10. Estimating factorization time

# 28 Explicit Galois realization of transitive groups of degree up to 15

Jürgen Klüners, Universität Heidelberg, Germany

Until now, the inverse problem of Galois theory, i.e., the question whether every finite group occurs as the Galois group of a field extension of $Q$, has not been solved. Even less is known in the direction of explicit results. Complete results for permutation groups of small degree were until now only known in degrees up to eleven. We encounter two types of problems. First, as mentioned above, not all the groups in the range were even theoretically known to occur as Galois groups over $Q$. Secondly, there arises the practical problem how to come from theoretical existence results to explicit polynomials. An important tool in the constructions is a Galois group program which also yields the correct ordering of the roots, as provided by the computer algebra system Kant.
For all transitive groups up to degree 15 we compute a polynomial $f \in Q[x]$ with $\mathrm{Gal}(f) = G$. We present different methods which allows us to realize nearly all of these groups. The few remaining cases are already studied in the literature or we give special solutions. Since complete tables are known up to degree 11, we specially look at transitive groups of degree 12-15. Most of the presented methods are independent of the ground field, but explicit computations have only been done for the ground field $Q$.
For nearly all transitive groups up to degree 15 we give a method to construct a polynomial over $Q$. These methods are suitable to construct regular extensions

of $Q(t)$ with prescribed Galois group, too. We discuss the remaining cases and prove that there exist regular extensions of $Q(t)$ for these groups. Altogether we prove that for all transitive groups $G$ up to degree 15 there exists a polynomial $f \in Q(t)[x]$ such that $\mathrm{Gal}(f) = G$ and the extension is regular.
This result is a joint work with G. Malle.

# 29 Function fields with a totally ramified prime at infinity

Sachar Paulus, KOBIL Computer GmbH, Worms, Germany

joint work together with S. D. Galbraith and N. P. Smart

The arithmetical situation in imaginary quadratic number fields is very special; we can observe there a behaviour which is very useful from a computational point of view. The most important property is the existence of a reduction theory which allows to compute for a given ideal a unique equivalent ideal. Thus, the whole arithmetic in such a field can be controlled. It is a major task to discover similar cases for other fields to understand the reason for this behaviour.
In the early 20s, Artin showed that exactly the same behaviour can be observed in imaginary quadratic function fields. More recently, the arithmetical connection between real and imaginary quadratic function fields was discovered bz Paulus/R"uck. The situation in function fields is very similar to the situation in number fields, except the fact that the splitting behaviour at infinity has some "freedom", i.e. depends on the chosen model. It was conjectured that the existence of a reduction theory is connected to the infinite prime being totally ramified (a case which, for number fields, does only occur for imaginarey quadratic fields).
In this talk, we present our results concerning arithmetic in function fields of arbitrary degree whose infinite prime is totally ramified. Is shows that not only there exists a unique ideal in every ideal class of smallest degree, but also a practical polynomial time reduction algorithm which is a natural generalization of Cantors algorithm in the imaginary qudratic case. Moreover, we present an analogue of the Number Field Sieve following Adleman, DeMarrais, Huang to solve problems in the ideal class group in subexponential time.
A further consequence of the infinite prime being totally ramified is that the ideal class group is a very handy presentation of the divisor class group of the certain curve. The resulting algorithms are independent of the field of constants and

thus also interesting for arithmetic algebraic geometry.
A full paper can be found on
http://www.informatik.tu-darmstadt.de/TI/reports

# 30 Chabauty and Covering Techniques

E. Victor Flynn, Liverpool, Great Britain

Given a curve $C$ of genus greater than 1, defined over a number field $K$, we consider the problem of trying to compute $C(K)$, the set of $K$-rational points on $C$. When the Jacobian group $J(K)$ has rank less than the genus of $C$, then there is a classical theorem of Chabauty, which guarantees that $C(K)$ is finite. Recently, this has been developed as a practical technique, using explicit equations for the formal logarithm on the Jacobian, and explicit embeddings of $C$ into $J$. This has led to the recent solution of several problems which can be rephrased in terms of finding $C(K)$ for some curve $C$; for example, the recent proof (Flynn, Poonen and Schaefer) that no quadratics over $Q$ have a $Q$-rational 5-cycle.
The question then arises as to what can be done when $J(K)$ has rank greater than or equal to the genus of $C$. Falting's Theorem still tells us that $C(K)$ is finite, but the current proofs of Falting's Theorem give no real hope of a practical technique. One avenue of attack is to try to find a collection of covering curves $D_1, ..., D_n$ such that $D_1(K), ..., D_n(K)$ cover $C(K)$, and then hope that Chabauty's Theorem is applicable to $D_1, ..., D_n$. One first chooses an Abelian variety $A$ (defined over $K$) such that there is an isogeny $f$ (also defined over $K$) from $A$ to $J$. One also tries to choose embeddings $C_1, ..., C_n$ of $C$ into $J$ such that $D_1, ..., D_n$, the pullbacks of $C_1, ..., C_n$ to $A$ under $f$, give $D_1(K), ..., D_n(K)$ as a cover of $C(K)$. This method of attack can be tried for any $C$, since there is always available the choice $A = J$, with $f$ taken to be a multiplication-by-$m$ map. In some cases, such as when $C$ is a bielliptic curve of genus 2, there are other choices of $A$ available. We describe several situations where this idea has been developed into a practical technique (joint work with Joe Wetherell), and several worked examples where this technique has been successfully applied to specific curves.

# 31 A kangaroo approach to function fields

Andreas Stein, Department of C & O, Waterloo, Canada

First, we compare optimized arithmetics in hyperelliptic function fields. Since every imaginary quadratic function field can be represented as a real quadratic function field over the same field of constants, it makes sense to consider the real case as a generalization of the imaginary case. It turns out that the group operation (multiply and reduce) in the imaginary case and the infrastructure operation (multiply and reduce) in the real case have precisely the same complexity. Whereas the increment operation (baby step) is by a factor of approximately $4g$ faster in the real case, where $g$ denotes the genus of the hyperelliptic curve. This means, as soon as baby steps apply effectively, one should use the arithmetic of real quadratic function fields. For instance, one can easily verify that the baby step giant step algorithm for computing class numbers and regulators is, asymptotically, by a factor of $4g$ faster in the real case. The main idea of the this algorithm is to approximate the divisor class number $h$ of the function field via truncated Euler products to obtain an estimate of the form

$$|h - E| < L^2 \ ,$$

and then search for a multiple of the regulator $R$ in the interval $[E - L^2, E + L^2]$ by $O(L)$ baby steps and giant steps. One clearly runs into space problems for larger values of $R$, since one has to store theoretically $O(L) = O(q^{(2g-1)/5})$ reduced ideals. This suggests to apply less space-consuming methods for computing invariants. Pollard's lambda method ("the method of catching kangaroos") fits perfectly into this context, since one can make use of the techniques to generate the interval $[E - L^2, E + L^2]$. This method generalizes to any algebraic function field given a way to compute the group operation in its Jacobian. It is possible to generalize this method to number fields as well. Stein and Teske (1998) showed how Pollard's lambda method can be applied to compute invariants of hyperelliptic function fields. On a computer with a single processor and enough space, baby step giant step is expected to be the faster method. One advantage of Pollard's lambda method is that it is very space-efficient. In addition, van Oorschot and Wiener (1994) provided an efficient parallelization of this method with linear speed-up. This parallelization and the improvements of Pollard (1998) can be generalized to function fields in a similar way. Thus, if one has access to a larger amount of computers and processors, these techniques provide us with an efficient tool to compute larger values of invariants. We provide examples for 25 digits class numbers which could be computed in less than two hours with the help of 40 SUN SPARC ULTRA 20.

## 32 Uniform Distribution of Recurrence Sequences Modulo Prime Powers

Tamas Herendí, Debrecen, Hungary

Some new results are developed for the examination of linear recurrences. If an integer prime $p$ and a linear recurrence sequence $u_n$ is given, then combining the new results with old ones, an explicite $t$ is determined, such that if the recurrence is uniformly distributed mod$p^t$, then it is uniformly distributed mod$p^s$ for any integer $s$, too.

## 33 Polynomial Factorization over $Q_p$ via the Zassenhaus Round Four Algorithm

David Ford, Concordia University, Montreal

The worst case of the round four algorithm leads to a search of potential exponential length. Strategies are discussed to avoid this search by (i) examining extended power series representations and (ii) Cantor-Zassenhaus techniques.

## 34 Polytopes and Polynomials

Shuhong Gao, Clemson University, USA

We study irreducibility and factorization of polynomials via their "shapes." A polynomial with $n$ variables is associated with a polytope in the $n$-dimensional Euclidean space, called its Newton polytope. When a polynomial factors, its polytope decomposes in the sense of Minkowski sum of integral polytopes. We present two general constructions of indecomposable polytopes, thus gives many infinite families of absolutely irreducible polynomials over an arbitrary field. Eisenstein's criterion is a special case of our result. We also present a polytope method for

factoring multivariate polynomials. Our method is most efficient for polynomials whose Newton polytopes do not have many decompositions. Illustration is given by an example.