# TAGUNGSBERICHT 21/1995
# COMPUTATIONAL NUMBER THEORY
## 28.05. – 03.06.1995

Die Tagung fand unter Leitung der Herren H.W. Lenstra Jr. (Berkeley), M.E. Pohst (Berlin) und H.G. Zimmer (Saarbrücken) statt.

Nach den sehr erfolgreichen ersten beiden Tagungen über „Computational Number Theory" in den Jahren 1988 und 1991 fand jetzt die dritte Tagung zu diesem Thema statt. Schwerpunkte waren diesmal Beiträge zu elliptischen Kurven, Modulformen und Arbeiten zur konstruktiven Klassenkörpertheorie.

Neben den Vorträgen im normalen Tagungsprogramm fanden an zwei Abenden zusätzlich informelle Sitzungen statt. Die erste Abendveranstaltung war der Präsentation der Computeralgebrasysteme Kash, Lidia, Magma und Pari gewidmet (andere Computeralgebrasysteme wie Simath kamen im regulären Vortragsprogramm bei entsprechenden Anwendungen zur Sprache). In der zweiten Abendveranstaltung, einer „Problem - Session", nutzten die Tagungsteilnehmer die Möglichkeit, Probleme aus ihrem eigenen Arbeitskreis in einem Plenum zu erörtern.

Die Tendenz zu weniger und dafür längeren Vorträgen erwies sich als ausgesprochen fruchtbar. Die ausgedehnten Pausen führten zu angeregten Diskussionen und boten die Möglichkeit zur Zusammenarbeit an konkreten Aufgabenstellungen. Dadurch wurden auch die Kontakte zwischen den Tagungsteilnehmern erheblich intensiviert, und vereinzelt führten Zusammmenarbeiten schon am Tagungsort zu ersten Resultaten.

**Vortragsauszüge:**

D.J. Bernstein:
**Multidigit modular multiplication with the explicit Chinese Remainder Theorem.**

Fix coprime moduli $m_1, \ldots, m_s$ of a few digits each. Let $n$ be an integer of a few hundred digits, We show how arithmetic modulo $n$ may be performed upon integers $u$ represented as vectors ($u \mod m_1, \ldots, u \mod m_s$). This method involves no multiprecision arithmetic, except in an easy precomputation; it is practical in software and extremely well suited for hardware. Our main tool is the explicit Chinese Remainder Theorem, which says exactly how $u$ differs from a particular linear combination of the remainders $u \mod m_i$.

W. Bley:
**Associated orders, local and global freeness**

Let $N/\mathbb{Q}$ denote a real abelian number field with group $G$. We denote by $U_N = \mathcal{O}_N^*/\{\pm 1\}$ the unit lattice in $N$. Then $U_N$ is in a natural way a $\mathbb{Z}[G]/T_G$–module, where $T_G = \sum_{g \in G} g$ denotes the trace element. This action extends to provide $U_N \otimes_{\mathbb{Z}} \mathbb{Q}$ with the structure of a $\mathbb{Q}[G]/T_G$–module. We define

$$\mathcal{A} = \{f \in \mathbb{Q}[G]/T_G \mid f(U_N) \subseteq U_N\}$$

to be the associated order of $U_N$, where as usual we identify $U_N$ with $U_N \otimes_{\mathbb{Z}} \mathbb{Z} \subseteq U_N \otimes_{\mathbb{Z}} \mathbb{Q}$. We now consider the following problems:

(1) explicit construction of $\mathcal{A}$,
(2) determination of the $\mathcal{A}$–module structure of $U_N$, in particular: is $U_N$ locally/globally free over $\mathcal{A}$,
(3) computation of a generating element $\epsilon \in \mathcal{U}_N$ such that $U_N = \mathcal{A} \cdot \epsilon$, provided that $U_N$ is globally free.

We present an algorithm that solves these problems, or at least reduces them to, admittedly, very hard problems in algorithmic number theory such as, for example, a principal ideal test. Note that this also gives a computational answer to the old question if there exists a Minkowski unit that together with its conjugates generates the unit group modulo torsion.

W. Bosma and J. Cannon:
**Programming with Algebraic Structures and Morphisms: The Magma Language**

The design of a Computer Algebra language is of necessity based on some particular view of mathematics. Analysis of systems such as Macsyma, Maple, Reduce and Mathematica show they are based on the idea of performing transformations on symbolic expressions belonging to a single fixed structure (usually some kind of differential ring). While this view may be appropriate for problems such as integration and the solution of differential equations, it is much less successful when used as the metaphor for computation in branches of mathematics such as algebra, number theory, geometry and combinatorics where the ideas of algebraic structure and structure-preserving transformation (morphism) are of fundamental importance.

A new model for the design of Computer Algebra systems based on the notions of algebraic structure (magma) and morphism has been devised. Magmas are first classified in terms of the algebraic variety to which they belong. The variety, of course, determines the operations and the axioms which these operations satisfy. However, to create a particular magma, we have to specify its (carrier) set and this is done through the notion of a category. For example, matrix rings, polynomial rings and power series rings are examples of (indexed) categories belonging to the variety of rings. Relationships between magmas (e.g. A is a submagma of B, C is a quotient magma of D) are then naturally represented in terms of morphisms.

Magma is a new software system for algebra, number theory and geometry which has been designed in accordance with these principles. The use of the concept of a magma as the design basis provides a natural strong typing mechanism. Further, structures and their morphisms appear in the language as first class objects. Standard mathematical notions are used for the basic data types. The result is a powerful, clean language which deals with objects in a mathematically rigorous manner. The effectiveness of the language for computation with number fields is illustrated with the calculation of the ideal class group of the octic field $\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{17})$ by elementary methods.

H. Cohen:
**Recent advances in the Pari package**

The aim of this talk was to give a survey of recent results obtained by the Bordeaux CNT group and mostly included in the recent release of the freely available Pari

package. In particular:

(1) basic element and ideal operations in number fields (E. Tollis),
(2) Round 4 algorithm, p–adic factorization (D. Ford, P. Letard),
(3) computation of the Dedekind $\zeta$ function, verification of GRH (E. Tollis),
(4) systematic computation of Galois groups up to degree $\leq 11$ (M. Olivier),
(5) finding all cubic fields in essentially linear time (K. Belabas),
(6) finding Galois automorphisms using p–adic LLL (H. C.),
(7) class and unit group computation (under GRH), principal ideal problem (H. C., F. Diaz y Diaz, M. Olivier),
(8) removal of GRH: certification (H. C., F. Diaz y Diaz, M. Olivier with help from R. Schoof and H.W. Lenstra),
(9) computations in relative extensions (H. C., F. Diaz y Diaz, M. Olivier),
(10) finding the explicit structure of $(o_{\mathcal{F}}/I)^*$ (H. C.),
(11) computing narrow and more generally ray class groups (H. C., F. Diaz y Diaz, M. Olivier).

Many tables and programs are available by ftp from megrez.math.u-bordeaux.fr.

J.-M. Couveignes:
**A few computations and arithmetic properties of covers of the sphere minus three or more points. Conics as moduli spaces.**

We first recall some equivalences of categories stressed by A. Grothendieck in his *Esquisse d'un programme* and give the definition of a *dessin d'enfant*. We give a famous theorem of Belyi and some improvement of ours stating that any curve $\mathcal{C}$ defined over a number field $\mathbb{K}$ carries a function $f$ unramified outside $\{0, 1, \infty\}$ and without automorphisms (i.e. $f \neq fa$ for any *non* trivial automorphism $a$ of the curve). Then having such a function being characteristic of a $\mathbb{K}$-isomorphism class of curves, it is natural to ask which kind of arithmetic information on $\mathcal{C}$ is given by the topological structure of the covering $f$. For example one knows that all primes of bad reduction of $\mathcal{C}$ (i.e. those primes $p$ for which there is no model of $\mathcal{C}$ with good reduction at $p$) must divide the order of the geometric Galois group of $f$. One may ask whether such primes must also divide the order of some geometric ramification order of $f$. In order to test such hypothesis we need a rather broad family of examples. We thus propose a construction of Belyi functions with no automorphisms on any genus zero curve defined over $\mathbb{Q}$. This construction goes as follows.

Let $m$, $n$, $p$, $q$ be four integers such that the sum over any subset of those four numbers is non zero. Let us call $C_{m,n,p,q}$ the curve in $\mathbb{P}_3$ given by the following equations

$$(1) \qquad ma + nb + pc + qd = 0$$
$$(2) \qquad ma^2 + nb^2 + pc^2 + qd^2 = 0$$

For any point $P = (a, b, c, d)$ in $\mathcal{C}_{m,n,p,q}$ we define the rational function

$$\phi_P(X) = (1 - aX)^m(1 - bX)^n(1 - cX)^p(1 - dX)^q.$$

We check that this function is ramified over the four values $\{0, 1, \infty, \lambda_{m,n,p,q}(P)\}$ where $\lambda_{m,n,p,q}(P) = \phi_P(\delta_P)$ and

$$\delta_P = \frac{(n+p+q).a^{-1} + (m+p+q).b^{-1} + (m+n+q).c^{-1} + (m+n+p).d^{-1}}{(m+n+p+q)}.$$

Thus the function $\lambda_{m,n,p,q} : \mathcal{C}_{m,n,p,q} \to \mathbb{P}_1$ is unramified outside $\{0, 1, \infty\}$. Furthermore we show that it has no automorphisms in general and that any genus zero curve defined over $\mathbb{Q}$ is isomorphic to some $\mathcal{C}_{m,n,p,q}$.

Also, the ramification multiplicities of $\lambda_{m,n,p,q}$ are 1 and 4 over 1, the sums of two numbers in $\{m, n, p, q\}$ over 0 and the sums of three numbers in $\{m, n, p, q\}$ over $\infty$. We even compute the monodromy of $\lambda_{m,n,p,q}$ and draw the corresponding *dessin*.

To finish with, we study the particular case $m = 1$, $n = 2$, $p = 3$, $q = 5$ and show that the corresponding curve $\mathcal{C}_{1,2,3,5}$ has bad reduction at 11 although all ramification multiplicities are smaller than 11 and thus prime to it.

We finish by noticing that ours $\mathcal{C}_{m,n,p,q}$ may be interpretated as moduli spaces of spheres minus four points *with multiplicities*.

J. E. Cremona:
**Infinite descent on elliptic curves**

In my talk I presented recent work of my PhD student Samir Siksek.

In the first part, I presented new bounds for the difference between the naive logarithmic height and the canonical height of points on an elliptic curve defined over a number field. In many cases, if not all, these improve on similar bounds obtained by Zimmer (1970s) and Silverman (1990). Three examples were provided, in which the bounds obtained were shown to be close to the best possible.

In the second part of the talk, I showed how to enlarge a set of $r$ independent points on an elliptic curve $E$ over a number field $K$ known to have rank $r$ (for instance, found by a 2-descent) to a $\mathbf{Z}$-basis for the full Mordell-Weil group $E(K)$. Here we first use estimates from the geometry of numbers applied to the Mordell-Weil lattice, in order to bound the index of the subgroup spanned by the known points (this has also been done by Gebel and Zimmer). We then use a sieving procedure to eliminate possible prime divisors $p$ of the index, by considering the image of $E(K)$ in $E(F_l)$ for a large number of auxiliary primes $l$. This was illustrated by two examples, including one of Mestre of rank 12, where it was shown that the 12 independent points given by Mestre span a subgroup of index 8 in the group $E(Q)$, and a basis for $E(Q)$ is determined explicitly.

M. Daberkow:
**On the explicit arithmetic computation of Hilbert class fields**

Based on a paper by Hasse on the construction of the Hilbert class field of $\mathbb{Q}(\sqrt{-47})$ in 1964 and on the proof of the existence theorem of class field theory by Kummer extensions we presented an algorithm for the construction of the Hilbert class field $H(\mathcal{K})$ for an arbitrary number field $\mathcal{K}$.

One can immediately reduce the problem to the construction of class fields to subgroups $\mathcal{C}$ of $Cl_{\mathcal{K}}$ such that $Cl_{\mathcal{K}}/\mathcal{C}$ is of prime order $p$. This construction is based on the fact that the class field to $\mathcal{C}$ is a subfield of the class field $\mathcal{E}$ of $\mathcal{F} = \mathcal{K}(\zeta_p)$ to $J = N^{-1}_{\mathcal{E}/\mathcal{F}}(\mathcal{C})$. Using $\{\mathfrak{a}_1\mathcal{H}_{\mathcal{F}}, \ldots, \mathfrak{a}_t\mathcal{H}_{\mathcal{F}}\} = \{\mathfrak{a}\mathcal{H}_{\mathcal{F}} \mid \mathrm{ord}(\mathfrak{a}\mathcal{H}_{\mathcal{F}}) = p\}$ with $\mathfrak{a}_i^p = \alpha_i o_{\mathcal{F}}$ and $U_{\mathcal{F}} = < \epsilon_0 > \times < \epsilon_1 > \times \ldots \times < \epsilon_r >$ we can show that the class field $\mathcal{E}$ of $\mathcal{F}$ to $J$ is of the form

$$\mathcal{E} = \mathcal{F}(\sqrt[p]{\mu_1}, \ldots, \sqrt[p]{\mu_n})$$

with $\mu_i \in \{\alpha_k \epsilon_0^{m_0} \cdot \ldots \cdot \epsilon_r^{m_r} \mid 1 \leq k \leq t, 0 \leq m_0, \ldots, m_r < p\} \setminus \{1\}$. Since the construction of $\mathcal{E}$ is very hard, we outlined the idea of the construction of a field $\mathcal{F} \subseteq S \subseteq \mathcal{E}$, such that the class field of $\mathcal{K}$ to $\mathcal{C}$ is a subfield of $S$, which can be computed.

At the end of the talk we gave some examples of Hilbert class fields, including the Hilbert class field of $\mathbb{Q}(\rho)$ for $\rho^4 - 5\rho^2 + 196 = 0$. Because of $Cl_{\mathbb{Q}(\rho)} \simeq C_3 \times C_3 \times C_4$, we have $[H(\mathbb{Q}(\rho)) : \mathbb{Q}] = 144$.

F. Diaz y Diaz:
**Computing the narrow class group**

Let $K$ be a number field of signature $(r_1, r_2)$. We denote as usual by : $\mathbb{Z}_K$ the integers ring, $E$ the unit group, $\mathcal{I}$ the invertible ideals, $\mathcal{P}$ the principal ideals, $\mathcal{H} \approx$

$\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$ the class group in the ordinary sense, $h$ the class number, $\mathcal{H}_2$ the group of classes of order $\leq 2$ and $\sigma_1, \ldots, \sigma_{r_1}$ the real embeddings of $K$ in $\mathbb{C}$.

The signature map sg : $K^* \to \mathbb{F}_2^{r_1}$ associated to $\lambda \in K^*$ the vector of $\mathbb{F}_2^{r_1}$ having components 0 when $\sigma_i(\lambda) > 0$ and 1 when $\sigma_i(\lambda) < 0$. An element $\lambda \in K^*$ is **totally positive** if $\mathrm{sg}(\lambda) = \underline{0}$. The class group and the class number in the narrow sense are $\mathcal{H}^+ = \mathcal{I}/\mathcal{P}^+$ and $h^+ = \#\mathcal{H}^+$, respectively, where $\mathcal{P}^+$ is the subgroup of $\mathcal{P}$ containing the ideals having a totally positive generator.

**Theorem** $H^+ = h \cdot 2^{r_1 - q}$, where $q$ is the rank of $\mathrm{sg}(E) \subset \mathbb{F}_2^{r_1}$.

For each class $C \in \mathcal{H}$ of even order $2m$ we define $\mathrm{sg}(C) = \mathrm{sg}(\beta)$ where $\mathfrak{a}^{2m} = \beta\mathbb{Z}_K$ for $\mathfrak{a} \in C$. This map is well defined as element of $\mathbb{F}_2^{r_1}/\mathrm{sg}(E)$.

Denote by $t$ the rank of $\mathrm{sg}(\mathcal{H}_2)$ in $\mathbb{F}_2^{r_1}/\mathrm{sg}(E)$. We have:

**Theorem** Let us denote by $s$ the 2-rank of $\mathcal{H}$ and by $s^+$ the 2-rank of $\mathcal{H}^+$. Then : $s^+ = s + r_1 - q - t$.

From a computational point of view, we determine the structure of $\mathcal{H}^+$ with the following algorithm :

**step 1.-** Construct the set $\mathcal{A} = \{\alpha_1, \ldots, \alpha_{r_1-q}, \varepsilon_1, \ldots, \varepsilon_q\}$, where $\varepsilon_1, \ldots, \varepsilon_q \in E$ gives a basis of $\mathrm{sg}(E)$ and $\alpha_1, \ldots, \alpha_{r_1-q} \in \mathbb{Z}_K$ gives a basis of the supplement of $\mathrm{sg}(E)$. Let $V \in \mathrm{GL}_{r_1}(\mathbb{F}_2)$ be the matrix of $\mathrm{sg}(\mathcal{A})$.

**step 2.-** From $\mathfrak{a}_1, \ldots, \mathfrak{a}_{s'}$, generators of $\mathcal{H}$, deduce elements $\beta_i$ such that $\mathfrak{a}_i^{n_i} = \beta_i\mathbb{Z}_K$ $i = 1, \ldots, s'$. Let $B'$ be the matrix whose columns are $\mathrm{sg}(\beta_i)$. Compute $B = V^{-1}B'$.

**step 3.-** Reduce to the Smith normal form (SNF) the matrix of relations

$$R = \begin{pmatrix} n_1 & & & & & \\ 0 & \ddots & 0 & & 0 & \\ & & n_{s'} & & & \\ & & & 2I_{r_1-q} & & 0 \\ & B & & & & \\ & & & 0 & & I_q \end{pmatrix}.$$

The SNF of $R$ gives the structure of $\mathcal{H}^+$ and provides a generator system for its cyclic groups.

E. V. Flynn:
**The Arithmetic of Hyperelliptic Curves**

We describe work in progess to develop techniques to perform the following.

(1) Find $J(\mathbb{Q})/2J(\mathbb{Q})$ via descent on $J$, the Jacobian of $C$.
(2) Deduce generators for $J(\mathbb{Q})$ via an explicit theory of heights.
(3) Apply local techniques to try to deduce $C(\mathbb{Q})$ via an embedding of $C(\mathbb{Q})$ inside $J(\mathbb{Q})$.

The first technique for (1) was due to Gordon and Grant which tries to compute the Mordell-Weil group $J(\mathbb{Q})$ by complete 2-descent for the highly special case when the curve of genus 2 has all of its Weierstrass points defined over $\mathbb{Q}$. We have developed and improved a method of descent by isogeny, and have also performed descents when there is no torsion on the Jacobian. All methods have been considerably enhanced during the last year, and many rank computations have been reduced from several days of computing time to a few seconds on the same machine. Step (2) is straightforward in principle, applying Hilbert's Nullstellsatz to the equations which describe the group law on a model of the Jacobian variety. In practice, the size of the polynomials in the resultant computations are too large. We have implemented improvements which use isogenies to improve the value of the height constants, and have computed generators for $J(\mathbb{Q})$ for several curves of genus 2. We have recently implemented step (3) for the case when the Jacobian of a curve of genus 2 has rank 1. In this case, it is possible to use the formal group over a local field to obtain a bound on the size of $C(\mathbb{Q})$. Experimentally, this bound seems typically to be strictly better than that obtained by Coleman's results on Chabauty's Theorem; indeed, in the 35 curves which we have so far considered, we have determined $C(\mathbb{Q})$ completely in all but one case.

I. Gaál:

**Power integral bases in algebraic number fields**

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 (dating back to Hasse) to decide if $K$ admits a **power integer basis**, that is an integer basis of the form $\{1, \alpha, \dots, \alpha^{n-1}\}$.

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

$$I(x_2, \dots, x_n) = \pm 1. \tag{3}$$

Hence the problem of determining power integral bases can be reduced to the resolution of the **index form equation** (3).

If $K$ is a cubic number field, the index form equation is a cubic Thue equation. I. Gaál and N. Schulte (1989) determined all power integral bases in totally real and also complex cubic number fields of small discriminants.

For quartic number fields the problem was considered by I. Gaál, A. Pethő and M. Pohst in a series of papers (1991–1994). It turned out, that the resolution of index form equations (3) in any quartic field can be reduced to a cubic Thue equation and to some corresponding quartic Thue equations. In addition, for special Galois groups we developed more efficient algorithms.

For higher degree number fields, the problem becomes more difficult because of the high degree and the number of variables in (3). It is only hopeful if the index form factorizes, which is the case if $K$ has proper subfields. For this reason we considered (3) in sextic fields with a quadratic subfield. In this case the index form equation (3) implies a cubic relative Thue equation over the quadratic subfield. For totally real cyclic sextic fields (I. Gaál, 1994) the corresponding equations are cubic inhomogeneous Thue equations. For totally complex sextic fields (I. Gaál, 1995) equation (3) reduces to some cubic Thue inequalities. For totally complex sextic fields with a quadratic subfield I. Gaál and M. Pohst (1995) gave an algorithm for the resolution of (3).

D. Kohel:
**On the category of supersingular elliptic curves**

The isogenies (including the zero map) from a supersingular elliptic curve $E'$ to a fixed supersingular elliptic curve $E$ can be equipped with a left $O = \mathrm{End}(E)$–module structure. The isomorphism class of $E'$ (over a field $k = \overline{k}$) is determined by the $O$–module structure of the collection of isogenies $E' \longrightarrow E$, and gives an equivalence of categories between supersingular elliptic curves over $k$ and the category of left projective $O$–modules of rank one. On considering the category of pairs $(E, \pi)$, where $E/\mathbb{F}_q$ and $\pi$ is the $q$–th power Frobenius endomorphism, one can describe purely algebraically the category of supersingular elliptic curves over $\mathbb{F}_q$.

D. Koppenhöfer:
**Monogeneity of quartic number fields**

Schya and Storch have studied the class of finite free $A$–Algebras $B$, where the variety Spek $(B)$ can be represented as a complete intersection in the projective space. In case of rank 3 and 4 this can be done in a canonical way; important examples are finite free extensions of Dedekind rings.

Starting from the rank 4 case, where Spek $(B)$ is represented by Proj $(C)$ with $C = A[T_0, T_1, T_2]/(F_1, F_2)$ a graded complete intersection, we give a simple criterion whether there exists a representation by a hypersurface algebra. A first step to find algebra generators $B$ is to find a representation by a hypersurface algebra in projective dimension one. The reduction of dimension is done via a Veronese transform, this works iff the corresponding Veronese variety contains, after a suitable coordinate change, the variety $\gamma(F_1, F_2)$.

Over the ring of integers of an algebraic number field as ground ring such coordinate changes are found by solving a diophantine equation with the cubic resolvent of $F_1, F_2$ as left hand side. Finally, from the hypersurface algebra representations all algebra generators can be found by solving Thue equations of degree 4.

The method has been implemented using KANT and has been applied to all totally real quartic number fields of discriminant $\leq 40000$.

F. Lemmermeyer:
**Explicit construction of 2-class fields**

Let $k$ be a quadratic number field with discriminant $d$; it is a classical result due to Redei, Reichardt, and Scholz that there is a cyclic quartic extension $K/k$ which is unramified outside $\infty$ if and only if there exist coprime discriminants $d_1$, $d_2$ such that $(d_1/p_2) = (d_2/p_1) = +1$ for all primes $p_j$ dividing $d_j$. Such an extension $K$ is always normal over $\mathbf{Q}$ and can be constructed by solving the diophantine equation $X^2 - d_1Y^2 = d_2Z^2$.

This result can be generalized by replacing the cyclic group of order 4 by certain non-abelian groups of order 8 and 16; as an example, the following theorem was given: If $k$ is a quadratic number field with discriminant $d$, then there is an extension $L/k$, normal over $\mathbf{Q}$, unramified outside $\infty$, such that $\mathrm{Gal}(L/k) \simeq H_8$ (the quaternion group of order 8) if and only if $d = d_1d_2d_3$, where the $d_j$ are coprime discriminants such that $(d_1d_2/p_3) = (d_2d_3/p_1) = (d_3d_1/p_2) = +1$ for all primes $p_j$ dividing $d_j$. If these conditions on the Legendre symbols are satisfied, then the corresponding extension $L$ can be constructed by solving an explicitly given system of three diophantine equations.

P.L. Montgomery:
**Square roots of products of algebraic numbers**

Let $\alpha$ be an algebraic number. Let $\gamma(\alpha) = \prod_{i=1}^{n} g_i(\alpha)$ be a product which we suspect is a nonzero square in $\mathbb{Q}(\alpha)$. We assume that the prime factorization of each $(g_i(\alpha))$ (and hence of $\gamma(\alpha)$) is known. In particular, each prime ideal should

have even exponent in $(\gamma(\alpha))$. Using this ideal factorization, we construct a square root of $\gamma(\alpha)$, if it exists. The algorithm uses lattice basis reduction to estimate a square root, successively replacing the problem by a simpler one until it can be done directly. Like the original $\gamma(\alpha)$, its constructed square root will have a product form. The algorithm generalizes to $k$–th roots for arbitrary $k > 0$.

V. Müller:
**LiDIA, a library for computational number theory**

LiDIA is a C++ library for computational number theory developed at the university of Saarbrücken. The LiDIA-group intends to develop software which is very efficient and easy to use. The first release of LiDIA was published in the February of 1995. It contains classes for doing multiple precision computations, e.g. work with modular numbers, rational numbers, floating point numbers and complex numbers. Moreover there exist classes for doing linear algebra over $\mathbb{Z}$, lattice reduction with the LLL algorithm and factoring integers using trial division and ECM. The first release is available per anonymous ftp on `crypt1.cs.uni-sb.de` in directory `pub/systems/LiDIA`. The next release will probably be published end of October 1995 and will contain an implementation of the PMPQS, a general polynomial class (including the FFT algorithm for polynomial multiplication over $\mathbb{Z}/m\mathbb{Z}$), a general matrix class, routines for counting the number of points on an elliptic curve modulo a prime $p$. Moreover we work on a class for algebraic numbers and a class for computations with binary quadratic forms. In addition to paper documentation, we will include a `html`-based online-documentation in the next release.

K. Nagao:
**On the construction of high–rank elliptic curves**

Mestre constructed elliptic curves over $\mathbb{Q}(T)$ with rank $\geq 11$. Modifying these curves, he also constructed elliptic curves over $\mathbb{Q}(T)$ with rank $\geq 12$. Now, we find a curve (over $\mathbb{Q}(T)$) with rank $\geq 12$ in the curves got by Mestre's construction with rank $\geq 11$ and modifying this, we obtain an elliptic curve over $\mathbb{Q}(T)$ with rank $\geq 13$. In the family of elliptic curves got by the specialization from high–rank curves over $\mathbb{Q}(T)$, we (with T. Kouya) find a curve over $\mathbb{Q}$ with rank $\geq 21$.

A. Odlyzko:
**Some curious power series coefficients**

G. Fee and A. Granville asked for the asymptotic behaviour of $a_n$, the coefficients of

$$f(z) = \prod_{k=1}^{\infty}(1-z^k)^{\mu(k)} = \sum_{n=0}^{\infty} a_n z^n.$$

G. Almkvist observed that for $150 \leq n \leq 10^4$, the signs of the $a_n$'s are periodic modulo 6, and that the $a_n$'s for n in any fixed residue class modulo 6 grow smoothly. The obvious question was whether this pattern persists. It does not, but the first counterexample is probably around $10^{11}$ or $10^{12}$. The exact behaviour of the $a_n$'s appears to be extremely complicated. It can be shown that the $a_n$'s are occasionally at least as large as $\exp(cn^{1/3})$. Upper bounds of similar magnitude can probably be obtained, but only by assuming the GRH and additional hypotheses on the distribution of zeros of Dirichlet L–functions.

J. Pila:
**Factoring integers with hyperelliptic curves**

I present a joint work with H.W. Lenstra, Jr. and Carl Pomerance on a probabilistic algorithm for factoring integers. Our algorithm is called the "hyperelliptic curve method", because it uses the Jacobian varieties of curves of genus two over finite fields in the same way that the elliptic method uses elliptic curves over finite fields.

While not a practical algorithm, the hyperelliptic curve method yields an improvement over previous complexity results for the detection of smooth numbers.

Our analysis of the hyperelliptic curve method has two main ingredients. The first is a new density theorem for smooth number in short intervals. The second is a theorem on the distribution of the order of the group of rational points on the Jacobian variety of a curve of genus two over a finite field.

A. van der Poorten:
**Curves with prescribed singularities**

The determinant $\Delta = \left|\binom{j_1}{i_1} x_h^{j_1-i_1}\binom{j_2}{i_2} y_h^{j_2-i_2}\right|$ arises in constructing polynomials $P(x,y)$ over $\mathbb{Z}$, so that all derivatives $P^{(i_1,i_2))}$ vanish at the $r$ conjugate points $(x_h, y_h)$. Here $\mathcal{K} = \mathbb{Q}(x) = \mathbb{Q}(y)$ has degree $r$ over $\mathbb{Q}$. The rows of the determinant are indexed by pairs $(i_1,i_2)$ and $h = 1,\ldots,r$. The $(i_1,i_2)$ lie in the 'triangle' defined by $0 \leq i_1 < k_{i_2}$ where $(k_i)$ is a (strictly) decreasing sequence of integers with $k_{d_2} = 0$. Columns are indexed by pairs $(j_1,j_2)$ with $0 \leq j_1 \leq d_1$, $0 \leq j_2 \leq d_2$. In a real constructiuon one is looking for factors common to all the maximal minors of a rectangular matrix with $M = (d_1+1)(d_2+1)$ columns and $N = r\sum k_i < M$ rows (generalising Cramer's rule in the case $N = M-1$). One studies the hyper–extreme case $N = M$ to the end. In a paper about to appear in **Experimental Mathematics** Bombieri and I mention

our finding that $\Delta$ factorises rather surprisingly in the case $r = 3$ as a product of a constant $c(k)$ depending on the 'triangle' $(k_i)$ and powers of differnce products of the $x_h$, respectively the $y_h$. The mysterious constant $c(k)$ is the $\sum k_i \times \sum k_i$ determinant

$$\left|\binom{j_1}{i_1}\binom{j_2}{i_2}\right|$$

with rows indexed by $(i_1, i_2)$ as above, and columns by the points in the 'lozenge' left by eliminating the triangle and its complement. For the special case $k_i = 2l(d_2 - 1)$ $(0 \le i \le d_2)$ where $d_1 = 3ld_2 - 1$ it is easy to prove a formula for $c_1$ if $d_2 = 1$. It is a complicate product of primes at most $d_1 = 3l - 1$. Remarkably, computations by David Hunt show that for general $d_2 = d$ one obtains

$$c_d = c_1^{\binom{d+2}{3}}.$$

We neither understand why $c_d$ should be a power of $c_1$ nor, given that it is some power, why it should be that particular power we find. Hunt also has 'discovered' formulas for general 'triangles' in the cases $d_2 = 2, 3$ and 4. We cannot prove any of them.

O. Schirokauer:
**General discrete logarithms**

Let $p$ be a prime number and let $q = p^n$. We address the problem of finding an algorithm which computes discrete logarithms in the finite field of cardinality $q$ and which has a running time of

$$L_q[1/3; c + o(1)] \qquad \text{for} \quad q\tilde{\mathcal{O}}\infty. \tag{1}$$

Both the function field sieve and the number field sieve have conjectured expected running times the size of (1), but only if one restricts the finite fields under consideration. In the case of the function field sieve, the restriction is to those $q$ for which $n \ge (\log p)^2$. For the number field sieve, the restriction is to those $q$ for which $n \le (\log p)^{\frac{1}{2}-\epsilon}$, where $\epsilon$ is any positive real number. Thus a gap remains.

In the case of the function field sieve, the constraint on $p$ and $n$ arises because the smoothness base in the polynomial ring over the prime field of $p$ elements must have size bounded by (1) and yet contain all irreducible, monic polynomials of degree less than or equal to some bound $B \ge 1$. In the case of the number field sieve, the constraint on $p$ and $n$ is necessitated by the appearance of many terms in the expression for the running time which are exponential in $n$. The largest of these is $(\log q)^{O(n)}$, which enters into the analysis, for instance, as the size of the discriminant of the number field used as a base field.

U. Schneiders:
**Estimating the 2-rank of cubic number fields by the Selmer group of the corresponding elliptic curves**

We determine a lower and an upper bound for the 2-rank of the class group of a non-Galois cubic number field $K$ generated by an irreducible polynomial

$$f(x) = x^3 + ax + b \in \mathbb{Z}[x].$$

The lower and upper bound arise from the construction of a subgroup of the 2-Selmer group and a group comprising the 2-Selmer group of the elliptic curve $E$ over $\mathbb{Q}$ defined by the Weierstrass equation

$$y^2 = f(x).$$

This result facilitates the construction of cubic number fields with class groups of large 2-rank. For instance, a cubic field $K$ of 2-rank 7 is obtained by the corresponding algorithm.

The estimates we derived generalize to a great extent a similar result obtained by Eisenbeis, Frey and Ommerborn [Computation of the 2-rank of pure cubic fields, Math. of Comp. 32, 1978, 559-569] in the special case of a pure cubic field $K$.

M. Schörnig:
**KASH – the KANT shell**

The software package for algebraic number theory KANT has been developed over the years by the research group of M.E. Pohst, firstly in Düsseldorf and now in Berlin. KANT is based on the software package MAGMA. It consists of a library of functions written in C, so the user had to have some knowledge of C to benefit from its functions. Because of this disadvantage we started to build a shell around the KANT library which is based on the user interface of the software package GAP. With this shell – called KASH – the user is now able to use the KANT functions (e.g. for the computation of maximal orders, unit and class groups, arithmetic in relative extensions of number fields) in a convenient environment.

After a brief introduction into the software–architecture of KASH and its datatypes, I explained some features and concepts :

- computation of subfields and their embeddings;

- the concept of the "move system", i.e. the automatic installation of homomorphisms between orders to allow the user to "move" algebraic elements between them and adjust their representation to the new basis;
- solution of Thue–equation;
- solution of (relative) norm–equations;
- programming language and user defined functions;
- the concept of PVM: PVM is public domain software for distributed computing. KASH posesses an interface to that software which is very easy to handle.

KASH can be obtained via ftp:
`ftp.math.tu-berlin.de /pub/algebra/Kant/Kash`

R. Schoof:
**Computing Twasawa modules of real quadratic fields**

Let $\mathcal{F}$ be a real quadratic number field of conductor $f$ and let $p$ be an odd prime. We present a method to systematically compute the $p$–class numbers of the fields $\mathcal{F}_n$ in the cyclotomic $\mathbb{Z}_p$–extension of $\mathcal{F}$. We can in particular verify the $p$–class group stabilize. As an illustration of our method we show the following.

**Theorem** For all real quadratic number fields $\mathbb{Q}(\sqrt{f})$ of conductor $f < 10000$ and $p = 3$ the Iwasawa $\lambda$–invariant vanishes.

The method exploits properties of the cyclotomic units in $\mathcal{F}_n$. If the prime $p$ is not split in $\mathcal{F}$, we can recover the structure of the $p$–class group:

$$A_n \simeq B_n \qquad \text{for } n >> 0$$

(here $A_n$ denotes the $p$–class group and $B_n$ the group of units modulo cyclotomic units of $\mathcal{F}_n$). If $p$ is split in $\mathcal{F}$ we have a somewhat weaker result.
Our methods apply to all real abelian number fields.

P. Serf:
**How to compute the rank of elliptic curves over real quadratic number fields of class number one**

We have developed and implemented general 2-descent over real quadratic number fields of class number one in order to determine the rank and points of infinite order of elliptic curves defined over such fields. General 2-descent applies to arbitrary elliptic curves, whether or not they have a non-trivial point of order 2. For $K = \mathbb{Q}$ the

method was described in [B&SD] ([B.J. Birch and H.P.F. Swinnerton-Dyer, *Notes on elliptic curves. I.*, J. Reine Angew. Math. **212** (1963), 7-25]) and implemented by J. Cremona in Exeter. The main difficulties when passing from $\mathbb{Q}$ to a real quadratic number field $K$ were to find

- a fundamental domain for the action of $Sl(2, \mathcal{O}(K))$ (where $\mathcal{O}(K)$ is the ring of integers of $K$) on the 2-dimensional complex upper half plane $\mathcal{H} \times \mathcal{H}$
- analogous versions of Lemma 3, 4, and 5 in [B&SD], containing sufficient criteria for the reduction of homogeneous spaces at primes of $K$ dividing the rational primes $p \neq 2, 3$, $p = 3$, and $p = 2$, resp.

Unfortunately, our program takes several hours of cpu time, even for curves with small coefficients and small rank defined over small number fields.

For elliptic curves with non-trivial 2-torsion, one can apply 2-descent via 2-isogeny, a method which goes back to Tate. 2-descent via 2-isogeny is much simpler than the general 2-descent, and the corresponding program only takes a few hundred seconds to compute the rank $r$ and $r$ linearly independent points for elliptic curves with medium-sized coefficients over medium-sized number fields.

As a by-product of the algorithm using 2-isogeny, we found 17 examples of Tate-Shafarevich groups with $2^{10}$ points of order 2 over real quadratic number fields when we computed the rank of

$$E_m : \; y^2 + xy = x^3 - 16mx^2 - 8mx - m$$

over $\mathbb{Q}(\sqrt{D})$ for $1 \leq m \leq 1000$ and $D \in \{2, 3, 5, 6, 7, 11, 13, 14, 17, 19\}$. (The family $E_m$ was taken from [K. Kramer, *A family of semistable elliptic curves with large Tate-Shafarevitch groups*, Proc. of the AMS **89,3** (1983), 379-386].)

R.J. Stroeker:

**Calculating integer points on elliptic Diophantine equations using elliptic logarithms**

In this talk the method of finding all integer points on a given model for an elliptic curve over $\mathbb{Q}$ is illustrated by means of the family of curves obtained by rewriting

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

in which a perfect square is expressed as the sum of consecutive cubes, in the more convenient form

$$y^2 = x^3 + d_n x,$$

with $d_n = \frac{1}{4} n^2 (n^2 - 1)$. An essential element of the method is the lower bound for

linear forms in elliptic logarithms recently obtained by Sinnou David. For $n$ in the range $2 \le n \le 50$ and $n = 98$ all points are found unconditionally.

One of the major advantages of the elliptic logarithm method is that it uses the structure and particulars of the Mordell–Weil group of the relevant curve. On the other hand, the construction of rank and generators is sometimes extremely hard. Advantages and disadvantages are illustrated by examples.

C. Thiel:
**Computing short representations of algebraic integers**

Let $F$ be an algebraic number field of degree $n$, let $O$ be an order of $F$ with integral basis $\omega_1, \dots, \omega_n$ and discriminant $D$. For $\xi \in F$ we denote by $\mathrm{H}(\xi)$ the maximum of the normalized archimedian valuations on $\xi$ and by $\mathrm{N}(\xi)$ the norm of $\xi$. Each $\xi \in F$ can be uniquely written in the form $\xi = \frac{1}{a_{n+1}} \sum_{i=1}^{n} a_i \omega_i$, where $a_1, a_2 \dots, a_{n+1}$ are rational integers, $a_{n+1} > 0$ and $\gcd(a_1, a_2 \dots, a_{n+1}) = 1$. We call $(a_1, a_2, \dots, a_{n+1})$ the *standard representation* of $\xi$ with respect to the given basis. The binary size $\mathrm{size}(\xi)$, i.e. the number of bits needed to write down the standard representation of $\xi$, is polynomially bounded by $\log \mathrm{H}(\xi)$ and $\log |D|$.

A *multiplicative representation* of $\xi$ is a pair $((\beta_1, \dots, \beta_\ell), (e_1, \dots, e_\ell))$, where $\beta_i \in F$ is given in standard representation, and $e_i$ is a rational integer for $1 \le i \le \ell$, such that $\xi = \prod_{i=1}^{\ell} \beta_i^{e_i}$. We explain how to multiply, divide and test equality of numbers given in a multiplicative representation in polynomial time, and prove

**Theorem** Given a multiplicative representation $((\alpha_1, \dots, \alpha_k), (f_1, \dots, f_k))$ of $\xi \in F$ we can compute another multiplicative representation $((\beta_1, \dots, \beta_\ell), (e_1, \dots, e_\ell))$ of $\xi$ such that

- $\mathrm{size}(\beta_i) = (n + \log |D| + \max\{|\log |\mathrm{N}(\alpha_j)|| \,:\, 1 \le j \le k\})^{O(1)}$,
- $\ell = \left(\sum_{j=1}^{k} \log |f_j| + \log\log \mathrm{H}(\xi) + \log |D| + \max\{|\log |\mathrm{N}(\alpha_j)|| : 1 \le j \le k\}\right)^{O(1)}$,
- $e_i \le \ell$,

in time

$$\left(n + \sum_{j=1}^{k} (\log |f_j| + \mathrm{size}(\alpha_j)) + \log |D| + \max\{|\log |\mathrm{N}(\alpha_j)|| \,:\, 1 \le j \le k\} + \log\log \mathrm{H}(\xi)\right)^{O(1)}.$$

E. Volcheck:
**Addition in the Jacobian of a plane algebraic curve**

We present an algorithm for addition in the Jacobian of a plane algebraic curve (represented as the divisor class group) over the rationals or a finite field.

Let $C$ be an absolutely irreducible plane algebraic curve of genus $g$ with a rational point $P_0$. We apply the Brill–Noether method of adjoints to compute $\mathcal{L}(D_1 + D_2 - gP_0)$ for $D_1, D_2$ effective divisors of degree $g$.

Improvements over a previous work by the author (Proc. Ants–1, Computing in the Jacobian of a plane algebraic curve) include

(1) using Hamburger–Noether expansions to represent places,
(2) determining adjoints via the formula "discriminant equals conductor times different", $< Fy >= \mathcal{CD}$,
(3) showing that the residual divisor can (essentially) be reduced to degree $g$.

L. Washington:
**Proving modularity of $\mathbb{Q}$–curves**

Ribet showed, under the assumption of Serre's conjectures, that an elliptic curve defined over a number field is modular if and only if it is a $\mathbb{Q}$–curve, namely an elliptic curve isogenous to its Galois conjugates. We show how one can actually in practice prove that a given $\mathbb{Q}$–curve is modular.

D. Zagier:
**Polylogarithms and multiple zeta values**

The polylogarithm functions $\mathrm{Li}_m(x) = \sum_{n=1}^{\infty} \frac{x^n}{n^m}$ ($m = 1, 2, \dots$ ; $\mathrm{Li}_1$ = usual logarithm) play an important role in several recent conjectures in number theory and algebraic K–theory. There are two main questions:

(1) linear relations (over $\mathbb{Q}$) among values $\mathrm{Li}_m(\alpha)$, $\alpha \in \overline{\mathbb{Q}}$,
(2) functional equations like the "S-term relation" (Spence, 1809)

$$\mathrm{Li}_2(x)+\mathrm{Li}_2(y)+\mathrm{Li}_2\left(\frac{1-x}{1-xy}\right)+\mathrm{Li}_2(1-xy)+\mathrm{Li}_2\left(\frac{1-y}{1-xy}\right) = \text{expr. involving } \mathrm{Li}_1$$

and for both it is important to find subgroups $G \subseteq F^\times$, where $F$ is either a number field or the function field $\mathbb{Q}(x, y, \dots)$, such that

(1) $\mathrm{rk}(G)$ is small, and
(2) $\sharp\{\alpha \in F^\times \setminus \{1\} \mid \alpha \in G \text{ and } 1-\alpha \in G\}$ is large.

Various theoretical and computational aspects of this problem were discussed.

A different (but related) set of questions concerns the "multiple zeta values"

$$\zeta(k_1,\dots,k_r) = \sum_{0<n_1<\dots<n_r} \frac{1}{n_1^{k_1}\cdot\dots\cdot n_r^{k_r}} \quad (k_i \in \mathbb{Z}^{\geq 1},\ k_r \geq 2)$$

which, like the polylogarithm functions, were first studied by Euler. The set of these numbers with given weight $k_1+\dots+k_r = k$ (there are $2^{k-2}$ of them) span a subgroup $R_k$ of $\mathbb{R}$ and the main question is to compute the rank of $R_k$ and the ring structure of $R = \bigoplus_{k\geq 0} R_k$ ($R_0 = \mathbb{Z}$). An algorithm was found to compute the slowly convergent multidimensional sums $\zeta(k_1,\dots,k_r)$ rapidly and to high accuracy; then LLL was used to find linear relations among them. There were many (e.g. there are 1024 $\zeta$'s of weight 12, but $\dim R_{12}$ is experimentally only 12); the experimental evidence suggests the formula

$$r_k = r_{k-2} + r_{k-3} \quad ; r_0 = 1,\ r_1 = 0,\ r_2 = 1$$

for $r_k = \mathrm{rk}(R_k)$. A theoretical upper bound, which is conjecurally the correct answer, can be derived. It reduces the question to a series of hard problems of linear algebra (over $\mathbb{Z}$), the first one being:
PROBLEM: Let $V_k$ be the space of homogeneous polynomials $f(x,y,z)$ of degree $k$ satisfying $f(x,y,z) + f(x,z,y) + f(z,x,y) = 0$ and $f^*(x,y,z) + f^*(x,z,y) + f^*(z,x,y) = 0$, where $f^*(x,y,z) = f(x,x+y,x+y+z)$. Determine the dimension (or better, a basis) of $V_k$.
The answer is 0 for $k$ odd and conjecturally $\lfloor \frac{k^2-1}{84} \rfloor$ for $k$ even.

M. Zieve:
**A New Class of Exceptional Polynomials**

An exceptional polynomial $f$ over a finite field $K$ is a separable polynomial that is a permutation polynomial over infinitely many finite extensions of $K$. An important problem is the classification of all exceptional polynomials. Since the composition of exceptional polynomials is exceptional, and conversely the composition factors of an exceptional polynomial are themselves exceptional, it suffices to study indecomposable exceptional polynomials. To each polynomial $f(x)$ over $K$, there is associated a group, the *geometric monodromy group* of $f$; it is the Galois group of $f(x)-t$ over $\overline{K}(t)$, where $\overline{K}$ denotes an algebraic closure of $K$. In 1993, Fried, Guralnick and Saxl (using, among other things, the classification of finite simple groups) derived severe restrictions on the possibilities for the geometric monodromy group $G$ of an indecomposable exceptional polynomial $f$. In particular, they showed that, with two

possible exceptions, $G$ must be an affine group and the degree of $f$ must be a power of the characteristic of $K$; every $f$ known prior to their work had these properties. The two exceptions are the subject of this talk. The work of Fried, Guralnick and Saxl left open the possibility that, for an indecomposable exceptional polynomial $f$, we could have $p = \mathrm{char}(K) = 2$ or 3, and $n = \deg f = p^k(p^k - 1)/2$, where $k \geq 3$ is odd; here $G$ is a group normalizing $PSL_2(p^k)$ in its transitive representation on $n$ points.

For $p = 2$, the first such polynomials were discovered by Müller in 1993; subsequently Cohen and Matthews discovered an infinite family of indecomposable exceptional polynomials over the field of two elements which, for each odd $k \geq 3$, contains polynomials having degree $2^{k-1}(2^k - 1)$ whose geometric monodromy groups are $PGL_2(2^k)$. I will discuss work done jointly with Hendrik W. Lenstra in the case $p = 3$. We have discovered an infinite family of indecomposable exceptional polynomials over the field of three elements which, for each odd $k \geq 3$, contains polynomials of degree $3^k(3^k-1)/2$ whose geometric monodromy groups are $PSL_2(3^k)$. Our methods also apply when $p = 2$, and give both a new way of discovering the polynomials of Müller, Cohen, and Matthews, and a new proof of their relevant properties.

H.G. Zimmer (joint with Josef Gebel and Attila Pethö):
**On Mordell's Equation**

The determination of all integral points on Mordell's elliptic curves

$$E_k: \qquad y^2 = x^3 + k \qquad (k \in \mathbb{Z},\ k \neq 0)$$

is a classical problem which was solved in many special cases. But no large scale computations have been carried through in the past. Our aim is to find all integral points on $E_k$ for $k \in \mathbb{Z}$ within the range

$$0 < |k| \leq 10000.$$

This can be done by a method proposed by Lang and Zagier. In fact the method of Lang and Zagier can be applied to an arbitrary elliptic curve $E$ over the rationals $\mathbb{Q}$ provided the rank and a basis of the group $E(\mathbb{Q})$ of rational points of $E$ over $\mathbb{Q}$ is known and an explicit lower bound for linear forms in elliptic logarithms can be given. The rank and a basis of the group $E(\mathbb{Q})$ can be determined by an algorithm of Manin which works under the assumption that the conjectures of Birch/Swinnerton-Dyer and Shimura/Taniyama are true. This algorithm was implemented by J. Gebel (see [1]). An explicit lower bound for linear forms in elliptic logarithms was obtained recently by S. David. On combining these two ingredients, we are able to compute all integral points on elliptic curves $E$ over $\mathbb{Q}$ of ranks $r \leq 6$ (see [2]). An application of our algorithm to Mordell's curves $E_k$ yields all integral points on $E_k$ for $0 < |k| \leq 10000$. These cuves are of ranks $r$ varying in the interval $0 \leq r \leq 4$ and they have up to 32 integral points.

Moreover, by using $p$-adic logarithms instead of elliptic logarithms, all $S$-integral points on $E_k$ for $0 < |k| \leq 10000$ can also be determined for any finite set $S$ of primes of $\mathbb{Q}$. This was carried out for $S = \{2, 3, 5\}$, and up to 94 $S$-integral points on $E_k$ were obtained.

The results are of interest in view of conjectures of Hall, Stark and Lang/Demjanenko concerning the number and size of integral point on elliptic curves.

[1] J. Gebel and H. G. Zimmer, Computing the Mordell-Weil group of an elliptic curve over $\mathbb{Q}$. In: Elliptic Curves and Related Topics, ed. by H. Kisilevsky and M. Ram Murty. CRM Proceedings and Lecture Notes, Amer. Math. Soc. 1994, 61 - 83.

[2] J. Gebel, A. Pethö and H. G. Zimmer, Computing integral points on elliptic curves. Acta Arith. **68** (2) (1994), 171 - 192.

Berichterstatter: M. Daberkow

Tagungsteilnehmer

Prof.Dr. Daniel J. Bernstein
3 Admiral Dr. # 362

Emeryville , CA 94608
USA

Prof.Dr. Henri Cohen
Mathematiques et Informatique
Universite de Bordeaux I
351, cours de la Liberation

F-33405 Talence Cedex

Dr. Werner Bley
Institut für Mathematik
Universität Augsburg

86135 Augsburg

Prof.Dr. Jean-Marc Couveignes
Laboratoire de Mathematiques
de l'Ecole Normale Superieure
U.R.A. 762
45, rue d'Ulm

F-75005 Paris

Wieb Bosma
Dept. of Mathematics
University of Sydney
School of Mathematics & Statistics

Sydney , NSW 2006
AUSTRALIA

Prof.Dr. John E. Cremona
Dept. of Mathematics
University of Exeter
North Park Road

GB-Exeter , EX4 4QE

Prof.Dr. Johannes Buchmann
Fachbereich Informatik - FB 14
Universität des Saarlandes
Postfach 151150

66041 Saarbrücken

Mario Daberkow
Fachbereich Mathematik
Technische Universität Berlin
Straße des 17. Juni 136

10623 Berlin

Dr. John Cannon
Department of Pure Mathematics
The University of Sydney

Sydney NSW 2006
AUSTRALIA

Prof.Dr. Francisco Diaz y Diaz
Mathematiques et Informatique
Universite de Bordeaux I
351, cours de la Liberation

F-33405 Talence Cedex

Prof.Dr. Eugene Victor Flynn
Dept. of Pure Mathematics
The University of Liverpool
P. O. Box 147

GB-Liverpool L69 3BX

Franz Lemmermeyer
Erwin-Rohde-Str. 19

69120 Heidelberg

Prof.Dr. David Ford
Department of Computer Science
Concordia University
1455 de Maisonneuve Blvd. West

Montreal Quebec H3G 1M8
CANADA

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

Berkeley , CA 94720
USA

Prof.Dr. Istvaan Gaal
Institute of Mathematics
Lajos Kossuth University
Pf. 12

H-4010 Debrecen

Prof.Dr. Jacques Martinet
Mathematiques et Informatique
Universite de Bordeaux I
351, cours de la Liberation

F-33405 Talence Cedex

David Kohel
Department of Mathematics
University of California
at Berkeley
942 Evans Hall # 3840

Berkeley , CA 94720-3840
USA

Prof.Dr. Peter L. Montgomery
Dept. Mathematics
Oregon State University

Corvallis , OR 97331-4605

Dr. David Koppenhöfer
Mathematisches Institut
Universität Tübingen
Auf der Morgenstelle 10

72076 Tübingen

Prof. Dr. Francois Morain
Laboratoire d'Informatique (Lix)
Ecole Polytechnique
Plateau de Palaiseau

F-91128 Palaiseau Cedex

Volker Müller
Fachbereich Informatik - FB 14
Universität des Saarlandes
Postfach 151150

66041 Saarbrücken

Jonathan Pila
6 Goldthorns Avenue

Kew East 3102
AUSTRALIA

Prof.Dr. Koh-ichi Nagao
Shiga Polytechnic College
1414 Hurukawa cho
Oh-mihachiman shi

523 Japan
JAPAN

Prof.Dr. Michael E. Pohst
Fachbereich Mathematik
Technische Universität Berlin
Straße des 17. Juni 136

10623 Berlin

Prof.Dr. Andrew M. Odlyzko
AT & T
Bell Laboratories
Room 2C-355
600 Mountain Avenue

Murray Hill , NJ 07974-2070
USA

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

North Ryde NSW 2109
AUSTRALIA

Prof.Dr. Michel Olivier
Mathematiques et Informatique
Universite de Bordeaux I
351, cours de la Liberation

F-33405 Talence Cedex

Prof.Dr. Reinhard Schertz
Institut für Mathematik
Universität Augsburg
Universitätsstr. 8

86159 Augsburg

Prof.Dr. Attila Pethö
Institute of Mathematics
Lajos Kossuth University
Pf. 12

H-4010 Debrecen

Prof.Dr. Andrzej Schinzel
ul. Brzozowa 12 m.24

00-286 Warszawa
POLAND

Prof.Dr. Oliver Schirokauer
Mathematics Department
Oberlin College

Oberlin OH 44074
USA

Prof.Dr. Roelof J. Stroeker
Econometrisch Instituut
Erasmus Universiteit
Postbus 1738

NL-3000 DR Rotterdam

Dr. Ursula Schneiders
Fachbereich 9 - Mathematik
Universität des Saarlandes
Postfach 151150

66041 Saarbrücken

Christoph Thiel
Fachbereich Informatik - FB 14
Universität des Saarlandes
Postfach 151150

66041 Saarbrücken

Martin Schörnig
Fachbereich Mathematik - FB 3
MA 8 - 1
Technische Universität Berlin
Straße des 17.Juni 136

10623 Berlin

Dr. Emil Volcheck
RISC (Research Institute for
Symbolic Computation)
Universität Linz

A-4040 Linz

Prof.Dr. Rene Schoof
Dipartimento di Matematica
2. Universita di Roma
"TOR VERGATA"

I-00185 Roma

Prof.Dr. Samuel S. Wagstaff
Department of Computer Sciences
Computer Science Building
Purdue University

West Lafayette , IN 47907-1398
USA

Pascale Serf
Fachbereich 9 - Mathematik
Universität des Saarlandes
Postfach 151150

66041 Saarbrücken

Prof.Dr. Lawrence Washington
Department of Mathematics
University of Maryland

College Park , MD 20742
USA

Prof.Dr. Hugh C. Williams
Department of Computer Science
The University of Manitoba

Winnipeg, Manitoba R3T 2N2
CANADA

Michael Zieve
Mathematisch Instituut
Rijksuniversiteit Leiden
Postbus 9512

NL-2300 RA Leiden

Prof.Dr. Jing Yu
Institute of Mathematics
Academia Sinica
Nankang

Taipei 11529
TAIWAN

Prof.Dr. Horst Günter Zimmer
Fachbereich 9 - Mathematik
Universität des Saarlandes
Postfach 151150

66041 Saarbrücken

Prof.Dr. Don B. Zagier
Max-Planck-Institut für Mathematik
Gottfried-Claren-Str. 26

53225 Bonn

**Notice:** E-mail addresses concerning this area can be obtained by Professor Odlyzko (**amo@research.att.com.**).