Math. Forschungsinstitut
Oberwolfach
E 20 /02122

MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

# Tagungsbericht 23/1988

## Konstruktive algebraische Zahlentheorie

22.5. bis 28.5.1988

Die Tagung fand unter der Leitung von Hendrik W. Lenstra Jr. (Berkeley), Michael Pohst (Düsseldorf) und Horst G. Zimmer (Saarbrücken) statt.

Gegenstand der Tagung waren neue Methoden und Ergebnisse der konstruktiven algebraischen Zahlentheorie. In 38 Vorträgen berichteten Mathematiker aus 10 Nationen über Forschungsergebnisse u.a. auf den Gebieten der algorithmischen Theorie der algebraischen Zahlkörper (Maximalordnungs-, Einheiten-, Klassengruppenberechnungen), der elliptischen Kurven und diophantischen Gleichungen, der konstruktiven Galois- und Gruppentheorie und über die Anwendung dieser Resultate auf schnelle Primzahltests und Kryptographie.

Ein zweiter Schwerpunkt der Tagung war die Präsentation spezieller Programmiersprachen und Softwaresysteme für die algorithmische Zahlentheorie.

Folgende Systeme wurden vorgestellt:

(1) KANT - eine Fortran Bibliothek für Rechnungen in algebraischen Zahlkörpern (Element- und Idealarithmetik, Algorithmen aus der Geometrie der Zahlen, Maximalordnungs- Einheiten- und Klassengruppenberechnungen) (Siehe Vortragsauszug U. Schröter).

Gefördert durch DFG Deutsche Forschungsgemeinschaft

©

(2) SIMATH - ein Computer Algebra System, das sowohl interaktiv (SIMCALC) als auch als C-Bibliothek benutzt werden kann und neben grundlegenden Algorithmen für ganze Zahlen, endliche Körper und Polynome auch spezielle Programme für Rechnungen in komplexen Strukturen, etwa Funktionenkörpern und Punktgruppen elliptischer Kurven enthält (Siehe Vortragsauszug M. Reichert).

(3) ALGEB - eine Pascal-ähnliche Programmiersprache, die die Benutzung beliebig langer Zahlen und besonderer Strukturen erlaubt (Siehe Vortragsauszug D. Ford).

(4) CAYLEY - ein Programmsystem für die konstruktive Gruppentheorie (Siehe Vortragsauszug J. Cannon).

(5) PARI - ein Softwaresystem für die Zahlentheorie, das auf 68020-Rechnern implementiert ist und z.B. arithmetische und transzendente Funktionen auswertet (Siehe Vortragsauszug Bernardi).

Die Vorführung dieser Systeme fand statt auf einem PC-MX2 und einem VICTOR (der Universität Saarbrücken), einem ATARI ST4 (der Universität Düsseldorf), zwei MACINTOSH II (des Forschungsinstituts), einem MC-5600 (bereitgestellt von der Firma MASSCOMP) und einer SUN 3/60 Workstation (bereitgestellt von der Firma SUN).

Im Laufe der Tagung konnten auf diesen Rechnern algorithmische Probleme, die sich aus der wissenschaftlichen Diskussion ergaben, z.T. unmittelbar gelöst werden. So wurde der erste Fall der Fermatschen Vermutung für die Primzahl 156 442 236 847 241 729 verifiziert, es wurden Einheiten berechnet, Indexformgleichungen gelöst, Kongruenzzahlen bestimmt...

In den Vorträgen und Computerdemonstrationen kamen alle Aspekte der algorithmischen Zahlentheorie zu Wort. Es zeigte sich, daß der Einsatz moderner Computer und konstruktiver Methoden wichtige neue Einblicke in die zentralen Probleme der Zahlentheorie ermöglichen.

Gefördert durch DFG Deutsche Forschungsgemeinschaft

## Vortragsauszüge

A.M. ODLYZKO:

### Zeros of the Riemann zeta function

A new algorithm, invented by A. Schönhage and the speaker, makes it possible to compute large sets of zeros of the Riemann zeta function much faster than with older methods. It has recently been implemented and it turns out to be very fast in practice as well as in theory. It has been used to compute almost 79 million zeros in the neighborhood of zero $10^{20}$, as well as several other large sets of zeros. These zeros all turn out to satisfy the Riemann hypothesis and provide evidence in favor of other conjectures that link the zeros of the zeta function to eigenvalues of random matrices.

M. HUANG:

### Recognizing primes in random polynomial time

A random polynomial time algorithm for recognizing the set of primes is presented. The techniques used are from arithmetic algebraic geometry, algebraic number theory and analytic number theory. The proof of the efficiency of the algorithm involves the classification and counting of the curves of genus 2 and their Jacobian over finite fields. The notion of good Weil numbers is introduced. It is proved that (1) for any good Weil number $\pi$ for a prime p, there exists an $F_p$-principally polarized Abelian variety A associated with $\pi$, and with the F-endomorphism ring $R = Z[\pi,\bar{\pi}]$. (2) Let

$\mathcal{D}$ = {R-ideal I: I is prime to p and the conductor of R, and
$I\bar{I} = \alpha R$ for some real $\alpha$}

$\forall\, I,J \in \mathcal{D}$, $\exists$ $F_p$ ppav $A_I$ with ring R and $F_p$-isogenous to A

$\forall\, I,J \in \mathcal{D}$, $A_I$ is $F_p$-isomorphic to A iff I is R-isomorphic to J .

Gefördert durch DFG Deutsche Forschungsgemeinschaft ©

It is proved that any 0-dim $F_p$-ppav associated with a good Weil number $\pi$ is the canonically polarized Jacobian of an $F_p$-curve of genus 2. It then follows that the number of $F_p$-isomorphic classes of $F_p$-curves of genus 2 whose Jacobian is associated with a good Weil number $\pi$ is at least the number of R-isomorphy classes in $\mathcal{D}$. It is then proved that the latter is at least $P^{1,5}/\log^c p$ for some constant c, for most good Weil numbers.

J. PILA

Generalization of Schoof's algorithm to Abelian varieties and applications

We describe a generalization to Abelian varieties over finite fields of Schoof's algorithm for elliptic curves. The algorithm computes the characteristic polynomial of the Frobenius endomorphism of the Abelian variety A over $\mathbb{F}_p$ in time $O_\Delta((\log p)^\Delta)$ where $\Delta$ depends only on the form of the equations defining A. The method, generalizing that of Schoof, is to use the machinery developed by Weil to prove the Riemann hypothesis for curves and Abelian varieties. As applications we show how to count the rational points on the reductions mod p of a fixed curve in time polynomial in $\log p$, and we show that, for a fixed prime l, we can compute the l-th roots of unity mod p, when they exist, in time polynomial in $\log p$.

K.S. McCURLEY

Algorithms for computing class numbers of imaginary quadratic fields

Let h(-d) be the number of equivalence classes of positive definite binary quadratic forms of discriminant -d. A new probabilistic algorithm is described for computing h(-d), with expected running time $O(L^c)$, where $L = \exp(\sqrt{\log d \log\log d})$. (A.K. Lenstra and C.P. Schnorr have suggested that $c = 1+o(1)$ should be possible). The algorithm

Gefördert durch DFG Deutsche Forschungsgemeinschaft ©

combines an approximation to h(-d) from the class number formula with a method for generating random relations on a set of generators for the class group. Similar ideas have been previously known to A.K. Lenstra, H.W. Lenstra, Jr., and C.P. Schnorr. In addition, an algorithm for computing discrete logarithms in the class group can be described, with expected running time $O(L^c)$, and the methods can be used to prove that the problems of computing h(-d) and the structure of the class group belong to the complexity class NP. This answers a question posed by E. Bach, G. Miller and J. Shallit.

H.C. WILLIAMS

Computational aspects of evaluating the class number of a real quadratic field

Several different computational techniques for evaluating the class number of a real quadratic field are briefly described. Also, the complexity of each method is given and possible generalizations discussed. If $\Delta$ is the discriminant of a quadratic field, the fastest unconditional algorithms determine the class number in $O(\Delta^{1/2-\epsilon})$ elementary operations; the fastest conditional methods compute it in $O(\Delta^{1/5+\epsilon})$ elementary operations. Finally, it is pointed out that under suitable Riemann hypotheses, it can be shown that the problem of calculating the class number and regulator of a real quadratic field is in class NP.

D. BUELL

Quadratic class groups and the Cohen-Lenstra heuristics

Let $d < 0$ be the discriminant of an imaginary quadratic field $Q(\sqrt{d})$, h its class number, and C its class group. Among the questions recently addressed by the heuristics of Cohen and Lenstra are these

(1) What is the frequency with which an odd prime p can be expected to divide h?

(2) What is the frequency with which the odd part of C is non cyclic?

Gefördert durch DFG Deutsche Forschungsgemeinschaft

(3) What is the frequency with which a given p-group is the p-SSG of C?

We have computed the ≈ 30 000 000 class groups of discriminant d for 0 <- d < 100 000 000 collecting such statistics as might be neccessary to test the Cohen-Lenstra heuristics for these questions. The data are in the main consistent with the heuristics, but a good statistical fit has so far not been possible.

U. SCHRÖTER

Computer number theory package

In my talk I presented the number theory package developed in Düsseldorf. There are more than 200 subroutines written in standard FORTRAN 77. The main algebraic topics implemented until now are: integral bases, algebraic integer arithmetic, ideal arithmetic, units (independent and fundamental), norm equations and class groups.

M. REICHERT

SIMATH, ein Computer-Algebra-System

SIMATH, i.e. SInix MATHematies, is a computer algebra system developed at the University of Saarbrücken on a Siemens PC MX-2.
We give the basic ideas of the system and an overview of the features of SIMATH:

developed for applications in constructive numer theory
open System, the sources will be available
higher level number theory algorithms
written in "C"
library of functions for use in "C"-programs
dialogue system, SIMCALC, i.e. SIMath, CALCulator, for interactive problem solving.

In the near future SIMATH will be available also on other computers such as SUN, Appollo and VAX.

Gefördert durch DFG Deutsche Forschungsgemeinschaft

D. ZAGIER

Polylogarithms and special values of zeta functions

The dilogarithm function $Li_2(x) = \sum_{n=1}^{\infty} \frac{x^n}{n^2}$ has many surprising properties and occurs unexpectedly in many places in mathematics. Some of these are discussed, e.g., the relationship of the identify $Li_2(\frac{3-\sqrt{5}}{2}) = \frac{\pi^2}{15} - \log^2(\frac{1+\sqrt{5}}{2})$ to an odd claim of Ramanujan about the near equality of two continued fractions. The deepest connection to number theory is that the value at s=2 of the Dedekind zeta-function of an arbitrary number field can be expressed in closed form in terms of the dilogarithm; for instance,

$$\zeta_{Q(\sqrt{7})}(2) = \frac{4\pi^2}{2i\sqrt{7}} [D(\frac{-1+\sqrt{-7}}{4}) - 2\ D(\frac{1-\sqrt{-7}}{4})].$$

This Theorem is related both to algebraic K-theory and to the theory of hyperbolic 3-manifolds. We also discuss the conjecture that $\zeta_F(m)$ for an arbitrary number field F and integer $m \geq 2$ can be similarly expressed in terms of the $m^{th}$ polylogarithm $\sum_{n=1}^{\infty} \frac{x^n}{n^m}$ with $x \in F$ and give examples in support of this conjecture for m=3 and F real quadratic.

A. PETHÖ

Representation of one by binary cubic forms with positive discriminants

We computed the solutions of the diophantine equations

$$x^3 - cxy^2 + dy^3 = 1 \qquad 0 < c \leq 30; \qquad 46 \leq c \leq 50$$
$$x^3 + x^2y - cxy^2 + dy^3 = 1 \qquad 0 < c \leq 20; \qquad c = 50$$
$$x^3 - ax^2y - bxy^2 + y^3 = 1 \qquad 1 \leq a \leq 60; \qquad 0 \leq b \leq a$$

with $|y| \leq 10^{41}$ under the condition that the discriminant $D_f$ of the polynomial is positive.
Summarizing the observations we conjecture the following connections

Gefördert durch DFG Deutsche Forschungsgemeinschaft

between cubic forms f(x,y) with $D_f > 0$ and the number of solutions $N_f$ of f(x,y)=1

| | $N_f$ | |
|---|---|---|
| f is not equivalent to a reversible form | 0 | |
| | 1 | |
| | 2 | |
| | 3 | f is equivalent to a reversible form |
| | 4 | |
| | 5 | |
| | 6 | , $D_f$ = 81, 148, 257, 361,? |
| | 7 | none |
| | 8 | |
| | 9 | $D_f$ = 49. |

Similar connection were proved by Delone (1930) and Nagell (1928) for cubic forms with negative discriminants.

C.P. SCHNORR

Perfect random number generators

A random number generator (RNG) is an efficient algorithm that transforms short random seeds into long pseudo-random strings. The concept of perfect random number generator has been introduced by Blum, Micali (1982) and Yao (1982). A RNG is perfect if it passes all polynomial time statistical tests, i.e. the distribution of output sequences cannot be distinguished from the uniform distribution of sequences of the same length.

We extend and accelerate the RSA-generator in various ways. We give evidence for more powerful complexity assumptions that yield more efficient generators. Let N = pq be product of two large random primes p and q and let d be a natural number that is relatively prime to $\varphi(N) = (p-1)(q-1)$. We conjecture that the following distributions are indistinguishable by efficient statistical tests:

the distribution of $x^d \pmod N$ for random $x \in [1, N^{2/d}]$.

the uniform distribution on [1,N].

This hypothesis is closely related to the security of the RSA-scheme.

Gefördert durch DFG Deutsche Forschungsgemeinschaft

Under this hypothesis we obtain a perfect random number generator that is almost as efficient as the linear congruential generator. We describe a method that transform every perfect random number generator into one that can be accelerated by parallel evaluation. Our method of parallelization is perfect, m parallel processors speed the generation of pseudo-random bits by a factor m; these parallel processors need not to communicate. Using sufficiently many parallel processors we can generate pseudo-random bits with nearly any speed. These parallel generators enable fast retrieval of substrings of very long pseudo-random strings.

D. FORD

The ALGEB programming language

The ALGEB language is an ALGOL derivative, designed specifically to facilitate the expression of the Zassenhaus round 4 maximal order algorithm. It is generally applicable to computations in algebra and algebraic number theory; it is particularly well-suited for computing in finite-dimensional $Q_p$-algebras.
ALGEB has now had three implementations:

1977: PDP-II

1986: VAX/VMS (native mode; virtual memory)

1988: IBM-PC

The VAX and IBM-PC versions are available at no cost from the author.

M.N. GRAS & G. GRAS

Necessary conditions for the existence of a relative power basis in algebraic number fields

Let E/F be a Galois extension of degree n, of Galois group G. Let H ge any nontrivial cyclic subgroup of G, order h. We prove, among other results:

Gefördert durch DFG Deutsche Forschungsgemeinschaft ©

Theorem: If $Z_E = Z_F[\theta]$, then for all a,b prime to h, there exists $\varepsilon_{a,b} \in Z_F^*$ s.t. for all prime P of E satisfying $H \subseteq G_{P,0}$ and $gHg^{-1} \subseteq G_{P,1}H$, $\forall g \in G$, the following congruence holds:

$$\varepsilon_{a,b} = \prod_{s \in S_P} \prod_{i=1}^{z(P)} \left( \frac{1-\gamma_P^{a\chi_P(s) f_P^i}}{1-\gamma_P^{b\chi_P(s) f_P^i}} \right)^{e(P)} \mod P,$$

with the following notations:

$\gamma_P = \pi_P^{\sigma_0 - 1}$, where $v_P(\pi_P) = 1$ and $<\sigma_0> = H$;

$f_P = |Z_F/P \cap Z_F|$; $z(P) = (G_{P-1} : G_{P,0})$; $e(P) = |G_{P,0}|$;

$\chi_P$ = the character $G \to (Z/hZ)^*$ defined by

$g \sigma g^{-1} \sigma^{-\chi_P(g)} \in G_{P,1}$, $\forall g \in G$, $\forall \sigma \in H$;

$S_P$ = {representative elements of right classes of G mod $G_{P,-1}$}

This result generalizes previous ones by M.N.Gras(J.N.T.,23,3(1986); Progress in Math.,63(1986)) and will be published in Publ.Math.Fac.Sci. Besancon (1988).

D.G. CANTOR

On arithmetical algorithms over finite fields

Standard methods for calculating over $GF(p^n)$, the finite field of $p^n$ elements, require an irreducible polynomial of degree n with coefficients in GF(p). Such a polynomial is usually obtained by choosing it randomly and the verifying that it is irreducible, using a probabilistic algorithm. If it isn't, the procedure is repeated. Here we we give an explicit basis, with multiplication table, for the fields $GF(_p p^k)$, for k = 0,1,2,..., and their union. This leads to efficient computational methods, not requiring the preliminary calculation of irreducible polynomials over finite fields and, at the same time, yields a simple recursive formula for irreducible polynomials which generate the fields.

Gefördert durch DFG Deutsche Forschungsgemeinschaft

The Fast Fourier Transform (FFT) is a method for efficiently evaluating (or interpolating) a polynomial of degree $< n$ at all of the nth roots of unity, i.e., on the finite multiplicative subgroups of F, in $O(n \log n)$ operations in the underlying field. We give an analogue of the Fast Fourier Transform which efficiently evaluates on some of the additive subgroups of F. This yields new "fast" algorithms for polynomial computation.

E. KALTOFEN:

Factoring into sparse polynomials

A new algorithm for factoring multivariate polynomials over a field of characteristic 0 is introduced. The algorithm takes as input an "oracle black box" that allowes to evaluate the polynomial at an arbitrary point. By proving this box it returns a program that allowes to evaluate the irreducible factors of the polynomial. The program fixes once and for all the enumeration and associates of these factors. It operates in a quadratic number of probes of the input box in terms of the total degree of the polynomial.
If one wants to obtain the sparse representation of one of the factors one can apply algorithms by Ben-Or & Tinrari and Zippel to the output program We show how this scheme is useful to check conjectures on factorization properties of determinants of Moufang loop tables or how to factor the u-resultant of a system of polynomial equations. These examples constitute some of the largest polynomials in number of terms (≈ 300 000 000) factored by computer today.

J. CANNON:

An overview of computational group theory

Computational group theory has developed rapidly over the past 20 years so that there currently exists a considerable number of algorithms for studying questions in the theory of permutation groups,

Gefördert durch DFG Deutsche Forschungsgemeinschaft

p-groups, soluble group, fp-groups and group representation theory. This talk mainly looked at algorithms for permutation groups. The notion of a base and strong generating set (BSES) provides the basis of almost all structural analysis of a permutation group. Current algorithms are either directly based on the ability to compute a BSES, (e.g. sequence stabilizer, normal closure), backtrack search (e.g. set stabilizer, centralizer) or homomorphism methods (e.g. Sylow p-subgroup).

J. MARTINET:

Small discriminants for a given permutation group

Let n be an integer and let G be faithful and transitive on n letters. Question: To construct extensions $E|Q$ such that:

(i) Gal $(F|Q)$ (F is galois closure of E) is isomorphic to G as a permutation group of degree n (Gal $(F|Q)$ acting on $Hom_Q(E, \bar{Q})$);

(ii) The conjugacy class of the infinite Frobenius is prescribed (up to the automorphisms of Gal $(F|Q)$ which fix E).

We recall some results on permutation groups, including 2-dimensional invariants, then discuss various methods of construction (geometry of numbers, class field and Kummer theory, embedding problems), and at last give examples for degree $\leq 8$. In particular, we give results on totally real sextic fields containing quadratic fields. (A table for such fields has been constructed for discriminant up to $5 \cdot 10^7$ by A.M. Bergé, M. Olivier and myself).

J. BUCHMANN:

Algorithms in algebraic number theory and their complexity

We discuss algorithms for computing maximal order, unit group and class group of an algebraic number field which are implemented in the software package for algebraic number theory in Düsseldorf. The maximal

Gefördert durch DFG Deutsche Forschungsgemeinschaft ©

order can be calculated by the round 2 algorithm of Ford and Zassenhaus. According to the analysis of H.W. Lenstra Jr. this algorithm is polynomial time equivalent to computing the largest square dividing an integer.
Unit and class group computation can be performed and analyzed using the general reduction theory of J. Buchmann and algorithmic ideas of Pohst and Zassenhaus.

H. COHEN:

Heuristics on class groups of number fields

In this joint work with Jacques Martinet, we generalize the Cohen-Lenstra heuristics in the following ways:

* Extensions can be of any degree
* Extensions can be non Galois
* The base field is arbitrary.

Extensive numerical examples are given in the January 1987 issue of Math. Comp.
One consequence is that, contrary to popular opinion, it is conjecturally not true that almost all quartic fields have as Galois group $S_4$: dihedral extensions represent a non zero proportion asymptotically.

J. Graf v. SCHMETTOW:

Class group computation in algebraic number fields

Subject of the talk was the algorithm for computing the class group structure invented by Pohst and Zassenhaus: Let $p_1,\ldots,p_\nu$ be those prime ideals of the algebraic number field whose norms are below the Minkowski bound $M_F$. Then $Cl_F \simeq Z^\nu/\Lambda$ where $\Lambda$ is the lattice of all exponent vectors $(C_1,\ldots,C_\nu) \in Z^\nu$ with $\Pi\, p_i^{c_i} \in H_F$. The algorithm determines a basis for $\Lambda$. In the first step, the prime numbers below $M_F$

Gefördert durch DFG Deutsche Forschungsgemeinschaft

are decomposed. In the second step, additional elements of $\Lambda$ are searched for and in the third step the basis of $\Lambda$ is derived by means of principal ideal testing. The implementation of the algorithm on Siemens 7.580-S, Atari ST4 and SUN 3/60 turns out to be very efficient for field degrees $\geq 8$.

F. DIAZ y DIAZ:

Construction explicite des extensions relatives

On décrit une méthode générale de construction explicite des extensions relatives $k|k'$ ou k est un corps de nombres ayant une degré et une signature fixées et dont le discriminant est borné en valeur absolue par une constante donnée.
Cette méthode semble bien adaptée pour le calcul de tables de corps de nombres imprimitifs.

H. ZASSENHAUS:

Arithmetic Structure of non commutative hypercomplex systems I

Given a Dedekind domain R with global quotient field F and a simple hypercomplex system A over F. How to embed a given R-order $\Lambda$ of A into hereditary R-orders, how to compute unit and class groups of $\Lambda$ ?
For preparation the center of $\Lambda$ considered as R-order of the center C(A) is embedded into the maximal-order of C(A). The aim of round 5 is to delay factorizations of discriminants and polynomials in the earlier rounds as much as possible. As a result an overorder defined as pseudo-Eisenstein over separable is obtained which is maximal if square factors have been eliminated.
For computations in $\Lambda$ a new index calculus is developed which requires only $O(n^2)$ steps in case $\Lambda = Z^{n\times n}$, both for addition and for multiplication.

Gefördert durch DFG Deutsche Forschungsgemeinschaft

W. BOSMA:

Improvements in primality testing

A theoretically simplified version of the Jacobi sum primality test (devised firstly by Cohen and Lenstra after Adleman, Pomerance and Rumely) leads to several practical improvements in the algorithm that is currently being implemented in Berkeley/Amsterdam (by M.P. van der Hulst). It is now possible to incorporate Lucas-Lehmer type tests in this general purpose algorithm. Other improvements on the Cohen-Lenstra version are e.g. that one can work in smaller ring extensions now and that some of the necessary (but expensive) powering can be combined.

B.W. MATZAT:

Neue Resultate aus der konstruktiven Galoistheorie

Unter Verwendung der bekannten Rationalitätskriterien für Galoiserweiterungen (siehe z.B. L.N.M. 1284) konnten neuerdings die Gruppen $PSp_4(p)$ für $p \equiv \pm 2 \bmod 5$ $(p \neq 2)$ von R. Deutzer (Berlin), die Gruppen 4 $PSU_3(p)$ für $p \equiv -1 \bmod 4$ von R. Nauheim (Karlsruhe) und G. Malle (Berlin), die Gruppen $F_4(p)$ für $p \equiv \pm 2, \pm 6 \bmod 13$ $(p \geq 19)$ von G. Malle und die sporadischen Gruppen $J_3$, $J_4$, Mc, Ru, Ly von H. Pahlings (Aachen) als Galoisgruppen regulärer Körpererweiterungen über $Q(t)$ nachgewiesen werden.

Experimente mit den neuen Zopfbahnenkriterien führten ferner erstmalig zur Darstellung der Gruppen $PSL_2(p^2)$ für $p = 5$ und $p = 7$ sowie der Mathieugruppe $M_{24}$ als Galoisgruppen regulärer Körpererweiterungen über $Q(t)$.

S.S. WAGSTAFF jr.:

A new bound for the first case of Fermat's last Theorem

We present an improvement to Gunderson's function, which gives a lower bound for the exponent in a possible counterexample to the first

Gefördert durch DFG Deutsche Forschungsgemeinschaft

case of Fermat's "Last Theorem" assuming that the generalized Wieferich criterion is valid for the first n prime bases. The new function increases beyond n = 29, unlike that of Gunderson. The first case of Fermat's "Last Theorem" has been proved for all exponents up to 156 442 236 847 241 729.

D. BERNADI:

The PARI library

The PARI library, designed by C. Betut, H. Cohen, M. Olivier in Bordeaux, and D. Bernadi in Paris, is a package running on machines equipped with a 68020 processor (presently SUN 3 and Macintosh II). It consists in I a core (more than 6000 lines of assembly language) implementing the basic operations on unlimited integers and real numbers with arbitrary precision. II a library, written in C, which give access to the following types: integers modulo another, fractional numbers (reduced or not), p-adic, complex, quadratic numbers, polynomials, power series, vectors, matrices, polynimials modulo another, rational fractions (reduced or not). The last types are recursive. A few fundamental arithmetic functions and many (real) transcendental functions are implemented. We plan to add more and also p-adic transcendental functions. One can use the library from a C or Pascal program. One can also use a so called "Super-Calculator" to use interactively the package.

L. WASHINGTON:

Large class numbers of real cyclotomic fields

We discuss a family of quintic polynomials discovered by Emma Lehmer. We show that the roots are fundamental units for the corresponding quintic fields. These fields have large class numbers and several examples are calculated. As a consequence, we show that for the prime p=641491 the class number of the maximal real subfield of the p-th cyclotomic fields is divisible by the prime 1566401.

Gefördert durch DFG Deutsche Forschungsgemeinschaft ©

E. BACH:

Some polynomials associated with Pollard's "Rho" method

Define polynomials $f_i$, $i = 0,1,\ldots$ by $f_0 = x$, $f_i = f_{i-1}^2 + y$. We show that $f_i - f_j$ factors in $Z[x,y]$ into absolutely irreducible polynomials. By associating a unique $p_{ij}$ (a factor of $f_i - f_j$) with each pair $i < j$ we find that for fixed $k$, $p \to \infty$

$$\Pr[\exists \text{ distinct } i,j < k \text{ with } f_i(x,y) \equiv f_j(x,y) \bmod p]$$

$$= \binom{k}{2}/p + O(1/p^{3/2})$$

when x and y are chosen at random from $Z/pZ$. If p is the smallest prime divisor of a composite number n, then the heuristic assumption that $p_{ij} = 0$ is a "random curve" implies that the least k for which

$$\exists i < k (\gcd(f_{2i+1} - f_i, n) \neq 1, n)$$

has expected value $\approx \sqrt{\pi/2} \cdot \sqrt{p}$ ; this was found by Pollard using a different heuristic argument.

F. HALTER-KOCH:

Principal factors in pure cubic fields

Let $K = Q(\sqrt[3]{a^2b})$ (a,b square-free, coprime) be a pure cubic field and R the product of the totally ramified primes. $\alpha \in O_K$ is called a principal factor (p.f.), if $|N(\alpha)| \mid R^2$, $|N(\alpha)| \neq 1$, $a^2b$, $ab^2$. Conditions on K to have a p.f. are discussed, and the p.f. are examined if they are minima (in the sense of geometry of numbers.)

B. BIRCH:

Hecke Actions on Ternary quadratic forms

The action of the Hecke algebra on the space $S^{(2)}$ of modular forms of weight 2 on $\Gamma_0(N)$ has been studied from many points of view. In this Lecture, a very simple Hecke action is suggested on the set X

Gefördert durch DFG Deutsche Forschungsgemeinschaft

of reduced positive definite ternary quadratic forms of determinant 2N. Write M(X) for the free module on X; then, viewed as a module over a Hecke algebra, M(X) appears to be essentially the same as the part of $S^{(2)}$ not fixed by the standard involution.

R. SCHOOF:

Elliptic curves

In 1987 A.O.L. Atkin devised a practical algorithm to count the number of points on an elliptic curve over a finite field, given by a Weierstrass equation. His algorithm is based on computations with the l-torsion points of the curve and on calculations on the modular curve. $X_o(l)$. It seems that Atkin can count the points on elliptic curves over $F_p$ where p is a prime up to 50 decimal digits.

J. McKAY:

Computing Galois groups

Lower bounds for Gal f are obtained from the theory of the Frobenius element giving shapes of elements of Gal f. Upper bounds are obtained from invariants. There exist infinitely many groups $G_1$, $G_2$ $G_1 \not\cong G_2$ with the same Brauer table (a bijective correspondence between character tables and class power maps) implying that spec R(x) = spec R'(x') for $x \Leftrightarrow x'$, $R \Leftrightarrow R'$. This implies that elementary Pólya combinations will not distinguish $G_1, G_2$. The method above is incorporated into Maple for deg $\leq 7$ (implemented by Ron Sommeling, Nijmegen).

J.S. CHAHAL:

Congruent numbers and elliptic curves

We give (in a closed form) a one parameter family $\{E_\lambda\}$ of elliptic curves over Q with each $E_\lambda$ of Q-rank at least one. We exhibit explicitly a point of infinite order and discuss its applications to the congruent number problem.

Gefördert durch DFG Deutsche Forschungsgemeinschaft ©

E. BECKER:

On the construction of large amicable numbers

The talk reports on the discovery of a pair of 526-digits amicable numbers. The idea behind the construction is a new type of a Thabit-rule (following W. Borho (1972)) which provides sufficient conditions for two numbers of the type $m_1 = g \cdot p^n \cdot \prod_1^k r_i \cdot (h_1 p^n - 1)$, $m_2 = q \cdot p^n \cdot c \cdot (h_2 p^n - 1)$ to be amicable.

G. CORNELL:

Constructing unramified extensions of fields containing many roots of unity

Let L = K(3n) be a field containing the $n^{th}$ following is an example: Suppose all the prime divisors of n split completely in K. Then the ray class field of K with conductor n is an unramified (at least at the finite primes) abelian extension of K(3n). This gives a fairly simple method of constructing examples of fields L = K(3n) whose class groups are large.

V.A. DEMJANENKO:

On the representation of numbers by binary forms

Let K be an algebraic number field of degree n, and let Z(K) be the ring integer number K.

Theorem. If

$$\Sigma_{i=o}^{m} a_i x^{m-i} y^i = C, \quad m \geq 3$$

$$a_o, a_1, \ldots, a_m, C, x, y \in Z(K),$$

then $H(P) < 2^{8m(m-1)(m-2)n} H_1^{(m-1)(m-2/2} H_2^{n/m}$

where

$$H(P) = \Pi_{j=1}^{n} \max\{|x^{(j)}|, |y^{(j)}|\}/|N(x,y)|,$$

$$H_1 = \Pi_{j=1}^{n} \max\{|a_o^{(j)}| \; |a_1^{(j)}|, \ldots, |a_m^{(j)}|\}/|N(a_o, a_1, \ldots, a_j)|,$$

$$H_2 = /N(D)/ \; (a_o, a_1, \ldots, a_m \; D)/, \; D = C/ \; (x,y)^m.$$

Berichterstatter: J. Buchmann

Gefördert durch DFG Deutsche Forschungsgemeinschaft

©

## Tagungsteilnehmer

Dr. L. M. Adleman
Department of Computer Science
University of Southern California

Los Angeles , CA 90089-0782
USA

R. Böffgen
Fachbereich 9 - Mathematik
Universität des Saarlandes
Bau 27

6600 Saarbrücken

Dr. E. Bach
Computer Science Department
University of Wisconsin-Madison
1210 W. Dayton St.

Madison , WI 53706
USA

W. Bosma
Mathematisch Instituut
Fakulteit Wiskunde en Informatica
Universiteit van Amsterdam
Roetersstraat 15

NL-1018 WB Amsterdam

Prof. Dr. E. Becker
Fachbereich Mathematik
der Universität Dortmund
Postfach 50 05 00

4600 Dortmund 50

Dr. J. Buchmann
Mathematisches Institut
der Universität Düsseldorf
Universitätsstraße 1

4000 Düsseldorf 1

Prof. Dr. D. Bernardi
Mathematiques
U.E.R. 48, Tour 45-46, 5eme etage
Universite Paris VI
4, Place Jussieu

F-75252 Paris Cedex 05

Dr. D. A. Buell
Institute for Defense Analyses
Supercomputing Research Center
4380 Forbes Boulevard

Lanham , MD 20706
USA

Prof. Dr. B. Birch
Mathematical Institute
Oxford University
24 - 29, St. Giles

GB- Oxford , OX1 3LB

Dr. J. R. Cannon
Department of Pure Mathematics
The University of Sydney

Sydney N.S.W. 2006
AUSTRALIA

Gefördert durch
DFG Deutsche Forschungsgemeinschaft
©

Prof. Dr. D. G. Cantor
20259 Inland Lane

Malibu , CA 90265
USA

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

Montreal Quebec H3G 1M8
CANADA

Prof. Dr. J. S. Chahal
Dept. of Mathematics
Brigham Young University

Provo , UT 84602
USA

Prof. Dr. G. Gras
Laboratoire de Mathematiques
Universite de Franche-Comte
Route de Gray

F-25030 Besancon Cedex

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

F-33405 Talence Cedex

Prof. Dr. M. N. Gras
Laboratoire de Mathematiques
Universite de Franche-Comte
Route de Gray

F-25030 Besancon Cedex

Prof. Dr. G. Cornell
Dept. of Mathematics
University of Connecticut
196, Auditorium Road

Storrs , CT 06268
USA

Prof. Dr. F. Halter-Koch
Institut für Mathematik
der Universität Graz
Halbärthgasse 1/I

A-8010 Graz

Prof. Dr. F. Diaz y Diaz
Mathematiques
Universite de Paris Sud (Paris XI)
Centre d'Orsay, Bat. 425

F-91405 Orsay Cedex

Prof. Dr. M. D. Huang
Department of Computer Science
University of Southern California

Los Angeles , CA 90089-0782
USA

Gefördert durch
DFG Deutsche Forschungsgemeinschaft
©

M. P. van der Hulst
Mathematisch Instituut
Fakulteit Wiskunde en Informatica
Universiteit van Amsterdam
Roetersstraat 15

NL-1018 WB Amsterdam

Prof. Dr. B.H. Matzat
Fachbereich Mathematik / FB 3
der Technischen Universität Berlin
Straße des 17. Juni 135

1000 Berlin 12

Prof. Dr. E. Kaltofen
Department of Computer Science
Rensselaer Polytechnic Institute

Troy , NY 12180-3590
USA

Prof. Dr. K. S. McCurley
Dept. of Mathematics
University of Southern California
University Park, DRB 306

Los Angeles , CA 90089-1113
USA

Prof. Dr. A. K. Lenstra
Department of Mathematics and
Computer Science, University of
Chicago, Ryerson Hall
1100 East 58th St.

Chicago , IL 60637
USA

Prof. Dr. J. McKay
Department of Computer Science
Concordia University
1455 de Maisonneuve Blvd. West

Montreal, Quebec H3G 1M8
CANADA

Prof. Dr. H. W. Lenstra, Jr.
Dept. of Mathematics
University of California

Berkeley , CA 94720
USA

Prof. Dr. A.M. Odlyzko
AT & T
Bell Laboratories
600 Mountain Avenue

Murray Hill , NJ 07974-2070
USA

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

F-33405 Talence Cedex

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

H-4010 Debrecen

Gefördert durch
DFG Deutsche Forschungsgemeinschaft
©

J. Pila
Dept. of Mathematics
Stanford University

Stanford , CA 94305-2125
USA

Prof. Dr. R. J. Schoof
Mathematisch Instituut
Rijksuniversiteit te Utrecht
P. O. Box 80.010

NL-3508 TA Utrecht

Prof. Dr. M. Pohst
Mathematisches Institut
der Universität Düsseldorf
Universitätsstraße 1

4000 Düsseldorf 1

U. Schröter
Mathematisches Institut
der Universität Düsseldorf
Universitätsstraße 1

4000 Düsseldorf 1

M.A. Reichert
Fachbereich 9 - Mathematik
Universität des Saarlandes
Bau 27

6600 Saarbrücken

Prof. Dr. Ch. Sims
Dept. of Mathematics
Rutgers University
Busch Campus, Hill Center

New Brunswick , NJ 08903
USA

J. Graf von Schmettow
Mathematisches Institut
der Universität Düsseldorf
Universitätsstraße 1

4000 Düsseldorf 1

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

West Lafayette , IN 47907
USA

Prof. Dr. C.P. Schnorr
Mathematisches Seminar
Fachbereich Mathematik
der Universität Frankfurt
Postfach 11 19 32

6000 Frankfurt 1

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

College Park , MD 20742
USA

Gefördert durch
DFG Deutsche Forschungsgemeinschaft
©

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

Winnipeg, Manitoba R3T 2N2
CANADA

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

5300 Bonn 3

Prof. Dr. H. J. Zassenhaus
Dept. of Mathematics
The Ohio State University
231 W. 18th Ave.

Columbus , OH 43210
USA

Prof. Dr. H.G. Zimmer
Fachbereich 9 - Mathematik
Universität des Saarlandes
Bau 27

6600 Saarbrücken

Gefördert durch
DFG Deutsche Forschungsgemeinschaft
©