04211 Abstracts Collection
Algorithms and Number Theory
— Dagstuhl Seminar —

John Cremona[1] and Michael E. Pohst[2]

[1] Univ. of Nottingham, GB
john.cremona@nottingham.ac.uk
[2] TU Berlin, DE
pohst@math.tu-berlin.de

Abstract. From 16.05.04 to 21.05.04, the Dagstuhl Seminar 04211 "Algorithms and Number Theory" was held in the International Conference and Research Center (IBFI), Schloss Dagstuhl. During the seminar, several participants presented their current research, and ongoing work and open problems were discussed. Abstracts of the presentations given during the seminar as well as abstracts of seminar results and ideas are put together in this paper. The first section describes the seminar topics and goals in general. Links to extended abstracts or full papers are provided, if available.

Keywords. Algorithmic number theory seminar at Dagstuhl

04211 Summary – Algorithms and Number Theory

This seminar on number-theoretical algorithms and their applications was the fifth on this topic at Dagstuhl over a period of more than 10 years. This time we attracted a record number of 54 participants from 14 countries.

One of the major goals of these seminars has been to broaden interactions between number theory and other areas. For instance, there has been an effort to bring together people developing the theory of efficient algorithms with people actually writing software.

There has also been continuing interest in cryptography, and almost a third of the talks were on algebraic curves, most with an eye to applications in cryptography. Since elliptic curves in cryptography seem to be mainly objects of hardware implementations, nowadays, the focus is on higher genus curves and related more sophisticated mathematical objects.

This time we also had a major new topic: algorithmic K-theory which has been rapidly developing over the last few years. Not surprisingly seven talks were given on this subject, several alone on (algorithmic aspects of) logarithmic class groups.

Most of the other talks focused on more classical topics of algorithmic algebraic number theory, with half a dozen on various aspects of solving Diophantine

equations. Among the variety of problems considered we just mention the computation of Picard groups and Drinfeld modules, but also quantum computing of unit groups. Several talks were on problems related to the development of number theoretical software.

The variety of topics was stimulating to the audience. The reaction of the participants was very positive and we believe that we succeeded in having an effective meeting that was able to appeal to a broad audience. We made sure to allow for adequate breaks between sessions, and there were many opportunities for discussions that the participants took advantage of. The pleasant atmosphere of Schloss Dagstuhl once again contributed to a very productive meeting.

Further information and abstracts: http://www.dagstuhl.de/04211/

Keywords: Algorithmic number theory seminar at Dagstuhl

Recent Developments in Computational Arithmetic Geometry

Nils Bruin (Simon Fraser University, CDN)

Computer algebra systems have recently become remarkably powerful tools for arithmetic geometric computations and experiments. In this talk, I will showcase some of the features that the MAGMA computer algebra system now offers. The MAGMA system is the result of the efforts of many talented mathematicians and programmers. While I will mainly be highlighting features that I have implemented in the past year, it is important to realise that these routines are heavily based on previous work of many others.

We start with a quick demonstration of the routines that MAGMA offers to compute with plane algebraic curves and their maps. As an example, we will compute a quotient of Klein's quartic $C : x^3y+y^3z+z^3x = 0$ by an automorphism subgroup and represent the quotient map.

Keywords: Computer algebra systems, MAGMA

Explicit Aspects of the Jacobi Inversion Problem

Jean-Marc Couveignes (University of Toulouse, F)

This talk is concerned with a question raised by R. Schoof which is beeing answered by B. Edixhoven with some advice or lemmata by Merkle, R. de Jong and myself. Fix a primitive modular cusp form f of level N, weight k : $f = \sum_{n\geq 1} a_n q^n$. For example one may take f to be the discriminant Δ which has level 1 and weight 12. In that case $a_n$is $\tau(n)$ the Ramanujan function. In general, f can be characterized by N, k and its kN^2 first coefficients. Given a prime p can one compute the coefficient a_p in polynomial time in $\log p$?

Keywords: Modular cusp form, Jacobi Inversion Problem

The XL-algorithm and a conjecture from commutative algebtra

Claus Diem (Universität Duisburg-Essen, D)

The XL-algorithm is an algorithm to solve overdetermined systems of polynomial equations which relies on a generalization of the well-known method of linearization. We show that a well-knwon conjecture from commutative algebra can be used to derive non-trivial upper bounds on the dimensions of the spaces of equations in the algorithm.

Keywords: Overdetermined systems of polynomial equations, upper bounds on the dimensions

Rational torsion on optimal curves

Neil Dummigan (University of Sheffield, GB)

Conjecture: Let l be a prime number. Let E' be an elliptic curve (over Q) of conductor N, and let E be the optimal (i.e. strong Weil) curve in the isogeny class of E'. If E' has a rational point of order l then so has E, except in some cases where l^2 divides N.

I would present some evidence from Cremona's tables, and sketch a proof of the case where N is squarefree and the reduction at at least one prime is split. I would also talk about results linking vanishing of the L-function with divisibility by l of the modular degree. I would say at least something about how this is all motivated by two different cases of the Bloch-Kato conjecture, and about further numerical evidence.

This talk would not be about algorithms as such, rather on some applications.

Keywords: Elliptic curve, modular degree

Montgomery scalar multiplication for genus 2 curves

Sylvain Duquesne (Univ. Monpellier, F)

Scalar multiplication is the basic operation in most cryptosystems based on the discrete logarithm problem. There exists old and efficient algorithms to do that, such as double and add. Traditional improvements of these algorithms are based on the minimization of the number of doubling and addition to be performed.

We present here another kind of algorithm which maixmize the number of operations but reduce the cost of each of them. For elliptic curves, the method consists in avoiding the computation of the y-coordinate, so that some computational saving are obtained. However, the addition of 2 points can only be done if the difference of these points is known.

Keywords: Montgomery scalar multiplication, hyperelliptic curves

The complexity of class polynomial computations via floating point approximations

Andreas Enge (Ecole Polytechnique - Palaiseau, F)

The exact complexity of computing generating polynomials for class fields of imaginary-quadratic number fields has so far received little attention in the literature. The invention of p-adic algorithms and their complexity analysis has motivated us to study the question more closely also for algorithms working with floating point approximations of complex numbers.

I will give a survey of the complexity of the well-known approaches and describe a new algorithm that is asymptotically optimal up to logarithmic factors in the class number.

Keywords: Complex multiplication, class field, complexity

Constructive Class Field Theory – Computing defining equations

Claus Fieker (University of Sydney, AU)

In this talk I presented algorithms for the explicit computation of defining equations for class fields (abelian extensions) of global function fields. After outlining methods that allow the computation of ray divisor class groups, I generalized the techniques used in the number field case to global function fields.

Unlike the number field case however, Kummer theory cannot be used in all cases to obtain generators for the field. For the missing case of cyclic extensions where the degree is a power of the characteristic, Artin-Schreier theory and generalisations hereof (rings of Witt vectors of finite length) are used.

Additionally I outlined how Hayes' approach to the computation of sign normalized Drinfeld modules of rank 1 and gave an explicit example comparing the two approaches: the algebraic approach from the number field side and the geometric one using Drinfeld modules.

Keywords: Class fields, algorithms for defining equations

Invariants for Genus one Curves

Tom Fisher (University of Cambridge, GB)

Let C be a smooth curve of genus one, defined over a field k. Let D be a k-rational divisor on C of degree n. (We assume that the characteristic of k does not divide 6n.) In the cases n=2,3,4, nineteenth century invariant theory gives formulae for the Jacobian of C. This observation was first made by Weil in the case n=2, and

has been described more recently in a paper of An, Kim, Marshall, Marshall, McCallum and Perlis.

I will describe my extensions of these results to the case n=5, and discuss some of the difficulties that currently prevent us treating larger values of n.

Keywords: Elliptic curves, invariants

Index-Calculus in Brauer Groups

Gerhard Frey (Universität Duisburg-Essen, D)

In the first part of the lecture we explained the Tate-Lichtenbaum pairing which relates the discrete logarithm in the group of points of order dividing a prime p of abelian varieties A over finite fields k with the elements of order dividing p in the Brauer group Br(K) of local fields K with residue field k. We continue to assume that K is a local field with residue field k.

Keywords: Brauer Groups, Tate-Lichtenbaum pairing, discrete logarithm in abelian varieties

Power Integral Bases - New Developments

Istvan Gaal (University of Debrecen, H)

It is a classical problem in algebraic number theory to decide if a number field admits power integral bases and if yes, to determine all possible generators of power integral bases.

The problem of determining generators of power integral bases is equivalent to solving the corresponding index form equation. Solving the index form equation is a hard computational task, especially for higher degree number fields. In the talk the following new developments were mentioned: An algorithm for solving index form equations in arbitrary sextic fields. The method takes very long CPU time but it is interesting that this problem can be dealt with using the presently known methods and their improvements. An efficient method was given for solving the p-adic index form equation in biquadratic number fields. The field index and all generators of power integral bases were determined in the infinite parametric family of simplest quartic fields. New criterion were given for the existence of power integral bases in composites of number fields. The above results are due to Y.Bilu, K.Győry, G.Nyul, P.Olajos and the speaker.

Keywords: Power integral basis, index form equation

Perfect Forms, cohomology of modular groups and the K-Theory of Z

Herbert Gangl (MPI für Mathematik, D)

Voronoi's reduction theory of positive definite quadratic forms over R of a fixed rank N, say, gives rise to a cell decomposition via perfect forms (these are forms of the above type which are characterized by their set of minimal vectors). The group $\Gamma = GL_N(Z)$ acts on this space, even when we add positive semi-definite forms with rational nullspace, and the quotient by the action of Gamma of the so extended space has been proved by Voronoi to be a finite cell complex.

We can compute the (in fact relative) homology of this complex for N=5 and N=6, using the well-known classification of perfect forms, together with the information on their neighbouring cells (all the necessary data have been provided by Jaquet). This allows us to determine (via Borel–Serre duality) the cohomology of Gamma with coefficients in Z[1/2,1/3,1/5] and Z[1/2,1/3,1/5,1/7] for N=5 and N=6, respectively.

Keywords: Cohomology of modular groups

Modular Equations for Generalized Weber Functions

Bill Hart (Leiden University, NL)

In this talk I will discuss the construction of modular equations for quotients of the Dedekind eta function, which have become known as generalized Weber functions.

Keywords: Weber functions, modular equations, Dedekind eta function

The GHS attack revised

Florian Hess (TU Berlin, D)

We discuss an extension of the GHS attack for elliptic curves in characteristic two, which considerably increases the number of curves for which the basic GHS attack was previously applicable.

Keywords: GHS attack, elliptic curves, hyperelliptic curves

Signed Digit Expansions in Elliptic Curve Cryptography

Clemens Heuberger (TU Graz, A)

Elliptic curve cryptography relies on the fact that multiples xP, where P is a point of an elliptic curve and x is an integer, can be computed quickly. This can be achieved using signed digit expansions for x.

In some cryptosystems, linear combinations $x^{(1)}P_1 + \cdots + x^{(d)}P_d$ have to be computed, where $P_1, \ldots, P_d$ are points on an elliptic curve and $x^{(1)}, \ldots, x^{(d)}$ are integers. We present algorithms (right to left and left to right) for computing such linear combinations quickly. We also consider window methods and related questions. The (online) left-to-right algorithms rely on an auxiliary expansion called the "alternating greedy expansion". A precise analysis for the algorithms is presented.

Keywords: Signed digit expansions, elliptic curve cryptography, sliding windows methods, joint sparse form, non-adjacent form, NAF, wNAF

Unit Equations

Istvan Jarasi (University of Debrecen, H)

Unit equations plays an important role in the theory of diophantine equations. In our talk we gave an overview of the present results on the number of solutions, on the height of the solutions and on the methods to compute explicitly the solutions of unit equations in two unknowns.

For unit equations in three or more unknowns at this time one has bounds only on the number of solutions, but we do not know anything on their height.

In our talk I gave a method to compute the "small" solutions of unit equations in three unknowns. (Here "small" means small height). This is really an extension of the method of Wildanger to determine the small solutions of unit equations in two unknowns.

The method was used to compute the "small" solutions of a norm form equation. There were also presented some improvements of the method used for norm form equations, and these improvements enabled us to compute the "small" solution of a resultant form equation.

Keywords: Unit equations

Computing Picard Groups of Orders in Global Fields

Jürgen Klüners (Universität Kassel, D)

Let K be a global field and O be an order of K. We develop algorithms for the computation of the multiplicative group of residue class rings for ideals in O. In general these orders are no Dedekind domains. Therefore there exist prime ideals such that the localization at these prime ideals is not a principal ideal domain.

Keywords: Picard Group, residue class rings, localizations

The $AGM - X_0(N)$ Algorithm

David R. Kohel (University of Sydney, AU)

The subject of p-adic point counting through canonical lifts was introduced by Satoh in 1999, later refined and specialized to $p = 2$ by Satoh, Skjernaa, and Taguchi and independently by Fouquet, Gaudry, and Harley. Subsequently, Mestre proposed a an efficient 2-adic AGM recursion in application to point counting. On careful inspection, one feature of the p-adic lifting phase of these algorithms is lifting of curve invariants, independent of the representative curve. The invariants are points on some modular curve, $X(1)$, the j-line, in the case of Satoh, or $X_0(8)$, in the case of Mestre's AGM as later refined by Gaudry and others to a univariate recursive Hensel lifting.

In the present work, I describe the generalization of these constructions to p-adic lifting of invariants on $X_0(N)$. The resulting points represent moduli of CM points, called Heegner points.

Keywords: P-adic point counting, modular curves

Cryptographic Applications of Trace Zero Varieties

Tanja Lange (Ruhr-Universität Bochum, D)

We present a kind of group suitable for cryptographic applications: the trace zero subvariety of the Jacobian of genus 1 or 2 curves. In the talk we show details on the efficient computation of scalar multiples. This is the main operation in cryptosystems based on the discrete logarithm problem. We give a theoretical comparison and implementation data for elliptic and genus 2 curves and for the trace zero variety of such curves for extension degrees 3 and 5.

Keywords: Trace zero varieties, cryptography

Solving Pell Equations via 2-Descent

Franz Lemmermeyer (Bilkent University - Ankara, TR)

The technique of 2-descent is used in the theory of elliptic curves for computing the rank and finding generators. It also provides concrete realizations of certain invariants of elliptic curves occurring in the conjecture of Birch and Swinnerton-Dyer. It is well known that there is a vague analogy between elliptic curves E and number fields K, where rational points on E correspond to units in the ring O_K of integers in K. I want to show here that the analogy becomes a lot closer if one concentrates on units in quadratic number fields, in other words: on integral solutions of the Pell equation.

Keywords: 2-descent, elliptic curves, units in quadratic number fields

What is the Logarithmic Class Group?

Hendrik W. Lenstra (Leiden University, NL)

The logarithmic class group $\tilde{Cl}(K)$ of a field K is the Galois group $Gal(K^{lc}/K^c)$. Here K^c is the composite of K with the unique $\hat{Z}$–extension of its prime field, and K^{lc} is the maximal extension of K^c in which all places of K^c split completely and that is abelian over K. Thus, for each non-trivial valuation v of K, the embedding of K into its v-adic completion K_v can be extended to a field homomorphism $K^{lc} \to (K_v)^c$, and K^{lc} is the maximal abelian extension of K with this property.

Keywords: K-Theory

Developing a System for Number Theory by Script Language — Announcement of the Release of NZMATH 0.1.1 —

Ken Nakamula (Tokyo Metropolitan University, J)

We are going to give neither mathematics nor algorithms, but a report of development of a new system NZMATH (New SIMATH) for Number Theory. We call for discussion on our policy and for joining the development. We shall describe what we learned from the development of SIMATH, why we employed the script language Python for NZMATH, who are the current members of development group, the present status and future aim of NZMATH, and how to participate in NZMATH. Though we might state frank opinions on the problems of existing systems, we are not denying SIMATH or other systems. We hope you to watch this baby NZMATH born in Japan warmly and severely as a new trial.

Keywords: SIMATH, script language, Python, NZMATH, CVS, the BSD license

Joint work of: Nakamula, Ken; Matsui, Tetsushi

The Discrete Logarithm in Logarithmic l-Class Groups and its Applications in K-Theory

Sebastian Pauli (TU Berlin, D)

We present an algorithm for the computation of the discrete logarithm in logarithmic l-Class Groups. This is applied to the calculation of the l-rank of the wild kernel $K_2(F)$ of a number field F. In certain cases it can also be used to determine generators of the l-part of $WK_2(F)$.

Keywords: Discrete logarithm, K-Theory, wild kernel

Joint work of: Pauli, Sebastian; Soriano-Gafiuk, Florence

The Principal Ideal Theorem

Reinhard Schertz (Universität Augsburg, D)

In the $p^n - th$ cyclotomic field $\mathbb{Q}_{p^n}$, p a prime number, $n \epsilon \mathbb{N}$, the prime p is totally ramified and the only ideal above p is generated by $\omega_n = 1 - \zeta_{p^n}$, with the primitive $p^n - th$ root of unity $\zeta_{p^n} = e^{\frac{2\pi i}{p^n}}$. Moreover these numbers represent a norm coherent set. A similar result can be established for the ray class field $K_{\mathfrak{p}^n}$ of conductor $\mathfrak{p}^n$ over an imaginary quadratic number field K where $\mathfrak{p}^n$ is the power of a prime ideal in K.

Keywords: Cyclotomic field, totally ramified prime, ray class field

Computations on Milnor K2 of Integer Rings

Romyar Sharifi (MPI für Mathematik, D)

Let R denote the ring $\mathbf{Z}[\mu_p, 1/p]$ for some odd prime p. We consider the Milnor K_2-group of the ring R.

Keywords: Milnor K2 group

Giving Baker's Theory a Modular Helping Hand

Samir Siksek (Sultan Qaboos University - Oman, SAS)

This talk is based on a series of papers where we combine the classical approach to diophantine equations (linear forms in logarithms, Thue equations, etc.) with a modular approach based on some of the ideas of Fermat's Last Theorem. This combination has so far been remarkably successful. We have been able to solve several outstanding diophantine equations including

$$F_n = y^m$$

where F_n is the n-th Fibonacci number, and

$$x^2 + 7 = y^m.$$

More details are found in the extended abstract (i.e. click the other icon)

Keywords: Baker's Theory, linear forms in logarithms, diophantine equations, level-lowering, modular approach, Fibonacci, Ramanujan-Nagell, exponential diophantine equations

Joint work of: Siksek, Samir; Bugeaud, Yann; Mignotte, Maurice

Efficient Solutions of Quadratic Equations

Denis Simon (Université de Caen, F)

I discuss the possibility of solving efficiently quadratic equations over Q.

Keywords: Quadratic equations

Computing Logarithmic Class Groups

Florence Soriano-Gafiuk (Université de Metz, F)

A new invariant of number fields, called group of logarithmic classes, was introduced by J.-F. Jaulent in 1994. The interest in the arithmetic of logarithmic classes is because of its applicability in K-Theory. Indeed this new group of classes is revealed to be mysteriously related to the wild kernel in the K-Theory for number fields. The new approach to the wild kernel is so attractive since the arithmetic of logarithmic classes is very efficient. Thus it provides an algorithmic and original study of the wild kernel. A first algorithm for the computation of the group of logarithmic classes of a number field F was developed by F. Diaz y Diaz and F. Soriano in 1999.

We present a new much better performing algorithm, which also eliminates the restriction to Galois extensions.

Keywords: K-Theory, wild kernel, logarithmic classes, positive divisor classes

Elliptic curves with a given number of points

Peter Stevenhagen (Leiden University, NL)

We discuss the following problem, which is an 'inverse problem' to the well known point counting problem for elliptic curves over finite fields. Given an integer n in N, find a finite field F_q and an elliptic curve E/F_q with $n = \#E(F_q)$.

Keywords: Elliptic curves, given number of points

$X^2 + Y^3 = Z^7$

Michael Stoll (IU - Bremen, D)

This equation is a special case of the Generalized Fermat Equation $x^p + y^q = z^r$. It is especially interesting since it is the extremal "hyperbolic" case: $\chi = 1/p + 1/q + 1/r - 1$ has the negative value closest to zero. For negative χ, it is known that the equation has only finitely many primitive integral solutions, and the closer χ is to zero, the more solutions are expected.

I will report on the proof (done jointly with Bjorn Poonen and Ed Schaefer) that the list of known primitive solutions is complete. The proof involves the explicit construction of ten twists of the Klein Quartic whose rational points cover the primitive solutions. This is done using ideas from the proof of Fermat's Last Theorem and a fairly recent result by Halberstadt and Kraus on twists of $X(7)$. In a second step, the set of rational points on each of these ten curves has to be determined. To achieve this, we set up a 2-descent on the Jacobian to determine the Mordell-Weil rank. In nine out of the ten cases, the rank is at most two, and Chabauty's method can be applied to find the rational points. In the last case, the rank is three, and we use a sieving argument on the Mordell-Weil group to rule out the existence of rational points leading to primitive solutions.

Keywords: Generalized Fermat Equation

A Polynomial Time Quantum Algorithm for the Computation of the Unit Group of a Number Field

Ulrich Vollmer (TU Darmstadt, D)

We present a polynomial time quantum algorithm for the computation of the unit group of algebraic number fields with finite degree over Q. The main technical tools are an extension of Shor's quantum Fourier transform technique to functions with irrational period lattices and a uniform choice of compact representations of generators of reduced ideals in the order considered. The proposed algorithms are a generalization of Hallgren's work which provably run in polynomial time.

Keywords: Polynomial time quantum algorithm, unit group of a number field

Joint work of: Vollmer, Ulrich; Schmidt, Arthur

Computing generators for the tame kernel of a global function field

Annegret Weng (Universität Mainz, D)

The examination of the order, structure and the generators of K_2 of the ring of integers of a number field F is still a field of active research.

The global function field case is much easier, since the order and structure of the kernel are well-known. In this talk, we discuss two methods for computing generators of the tame kernel of a global function field using ideas of Bass, Tate, Groenewegen, Belabas und Gangl.

Keywords: K-theory, function field, tame kernel

Beilinson's conjecture for K₂ of certain (hyper)elliptic curves

Rob de Jeu (University of Durham, GB)

We verify Beilinson's conjectures about K_2 for curves for curves of genus 2, 3, 4 and 5 in certain families of hyperelliptic curves defined over the rationals. For one of those families we can show that the rank of the integral part of K_2 for most curves in it is at least g, for arbitrary genus g, by establishing a limit formula for the Beilinson regulator.

Keywords: Beilinson's conjectures, elliptic curves, hyperelliptic curves

Joint work of: Dokchitser, Tim; de Jeu, Rob; Zagier, Don;

Finding prime values of a polynomial which represents all the primes

Herman te Riele (CWI - Amsterdam, NL)

Jones, Satoh, Wada and Wiens (The Amer. Math. Monthly 83 (1976), 449-463) have given a polynomial P(a,b,...,z) of degree 25 in the 26 variables a,b,..,z, having the property that as its variables range over the non-negative integers, the set of **positive** values which this polymomial assumes is precisely the set of primes. For the explicit form of this polynomial we refer to the paper mentioned above. Unfortunately, finding negative values of this polynomial is much easier than finding positive values.

Keywords: Prime values