09221 Abstracts Collection
Algorithms and Number Theory
— Dagstuhl Seminar —

Johannes A. Buchmann[1], John Cremona[2] and Michael E. Pohst[3]

[1] TU Darmstadt, D
buchmann@cdc.informatik.tu-darmstadt.de
[2] University of Warwick, GB
John.Cremona@gmail.com
[3] TU Berlin, D
pohst@math.tu-berlin.de

Abstract. From 24.05. to 29.05.2009, the Dagstuhl Seminar 09221 "Algorithms and Number Theory " was held in Schloss Dagstuhl – Leibniz Center for Informatics. 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. Algorithms, Number Theory, Cryptography

09221 Executive Summary – Algorithms and Number Theory

This seminar on number-theoretical algorithms and their applications was the sixth on this topic at Dagstuhl over a period of seventeen years. This time 39 people from 10 countries participated.

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. These aspects were both emphasized by the topics of special interest in this year: Number Theoretical Software and Algorithms for the Post Quantum Era.

About half of the 24 talks given were in these areas showing rapidly growing interest. One fourth of the talks were on curves, most with an eye to applications in cryptography.

The other talks focused on more classical topics of algorithmic algebraic number theory. We just mention the calculation of global fields and of class groups.

Dagstuhl Seminar Proceedings 09221
Algorithms and Number Theory
http://drops.dagstuhl.de/opus/volltexte/2009/2128

Even though we had less participants than at the last meeting the group seemed to be more homogenous. The variety of topics of the talks was stimulating to the audience. Their smaller number gave more room for discussions. It did not come as a surprise that these were most intensive in our emphasized topics.

For example, number theoretical software was not only discussed but also developed during the meeting. The participants did indeed a lot of coding. We would like to mention hat M. Stoll has a C program called ratpoints which is very fast at finding rational solutions to $y^2 = f(x)$. During the conference this program was incorporated into Sage, a process which included finding several bugs (memory leaks) in ratpoints so that M. Stoll could fix them right there.

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 - as already metioned - 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. Even more positively, several younger people who were there (for the first time) told us that they not only found it a very good meeting indeed, but the best venue they had been to for a conference.

Joint work of: J. Buchmann (Darmstadt), J. Cremona (Warwick), M. E. Pohst (Berlin)

The new GP interpretor and other recent improvements in PARI/GP

Bill Allombert (Université Montpellier II, FR)

We present some recent improvement of the PARI/GP computer algebra system, in particular the rewrite of the GP interpretor as a combined bytecode compiler/bytecode evaluator, the new GP debugger, a dedicated type for finite fields elements, algorithms for elliptic curves over finite fields including SEA, a port of Nguyen/Stelhé LLL^2 lattice reduction algorithm, and the GALPOL database of polynomials defining Galois extensions of the rationals.

Code-based post-quantum cryptography

Daniel Bernstein (University of Illinois - Chicago, US)

McEliece's code-based cryptosystem was introduced in 1978 and is one of the leading candidates for post-quantum public-key cryptography. All known attacks against the cryptosystem, including attacks by quantum computers, take time exponential in the code length, while encryption and decryption take polynomial time with very small exponents.

This talk will explain (1) how the original parameters proposed by McEliece were broken in 2008 by Bernstein, Lange, and Peters, (2) the computational issues that arise in using the cryptosystem for larger parameters, and (3) how list decoding of Goppa codes is connected to the Lenstra–Konyagin–Pomerance–Coppersmith–Howgrave-Graham–Nagaraj algorithm to find divisors in residue classes.

Joint work of: Daniel Bernstein; large parts are joint work with Tanja Lange and Christiane Peters

See also: http://pqcrypto.org/code.html

Sage - a platform for computational number theory

Robert Bradshaw (University of Washington, US)

Sage is a free open-source mathematics software system. It combines the power of many existing open-source packages into a common Python-based interface, together with nearly a million lines of new code. It aims to be a viable free open source alternative to Magma, Maple, Mathematica and Matlab. In this talk I focus on using Sage to answer questions related to elliptic curves, number fields, and lattices.

Some Recent Developments in Magma

Steve Donnelly (University of Sydney, AU)

This will be an overview of developments in Magma that are of interest to number theorists.

Some of the principal topics will be: modular forms of various flavours (including Hilbert modular forms), tools for elliptic curves over global fields (such as the Cassels-Tate pairing), and routines for lattice reduction and enumeration.

CM - Software for complex multiplication

Andreas Enge (Ecole Polytechnique - Palaiseau, FR)

Floating point approximations remain the approach of choice for constructing elliptic curves with complex multiplication, or more generally class fields of imaginary-quadratic number fields.

I present on-going work on publishing my implementation as free software, including helper libraries for the arithmetic of complex numbers and of polynomials over floating point numbers.

Full Paper:
http://www.multiprecision.org/

Pairings from small degree functions

Florian Hess (TU Berlin, DE)

The Weil and Tate-Lichtenbaum pairings on elliptic curves play an import role in cryptography. The efficient computation of (modifications of) these pairings is effected by the evaluation of suitable rational functions. We discuss a convenient framework that essentially encompasses all previously known such rational functions and provides new functions of smallest possible degree. We also give an interpretation in terms of class field theory.

Keywords: Tate and Weil pairing, elliptic curves, cryptography

Tabulating Class Groups of Quadratic Fields

Michael J. Jacobson (University of Calgary, CA)

Class groups of quadratic fields have been studied since the time of Gauss, and in modern times have been used in applications such as integer factorization and public-key cryptography. Tables of class groups are used to provide valuable numerical evidence in support of a number of unproven heuristics and conjectures, including those due to Cohen and Lenstra. In this talk, we discuss recent efforts to extend existing, unconditionally correct tables of both imaginary and real quadratic fields. After a brief summary of the state-of-the-art in the imaginary case, we will discuss recent efforts to extend tables in the real case. This includes incorporating ideas of Sutherland for computing orders of elements in a group, as well as constructing an unconditional verification algorithm using the trace formula of Maass forms based on ideas of Booker. This is joint work with Matt Greenberg, Andrew Shallue, and Hugh Williams.

Keywords: Quadratic field, class group tabulation

CM invariants in dimension 2

David R. Kohel (CNRS - Marseille, FR)

Algorithms for constructive complex multiplication of elliptic curves have seen research on various fronts: using complex analytic, p-adic, and CRT algorithms for determining CM points, and suitable choice of moduli space and functions for producing class polynomials of small height. We discuss analogous questions for complex multiplication of abelian surfaces. In particular, we construct invariants of Richelot isogenies which provide candidates for constructing class invariants smaller than the Igusa invariants of level 1.

Keywords: Complex multiplication, abelian varieties

Pairings on Edwards curves for cryptography

Tanja Lange (TU Eindhoven, NL)

Since their introduction to cryptography by Bernstein and Lange, Edwards curves have received a lot of attention because of their very fast group law. The group law in affine form was introduced by Edwards along with a description of the curve and several proofs of the group law. Remarkably none of the proofs provided a geometric interpretation of the group law while for elliptic curves in Weierstrass form the explanation via the chord-and-tangent method is the standard.

It was mostly for this lack of a geometric group law that Edwards curves were considered unsuitable for pairing computations and indeed all attempts to develop explicit formulas for pairing computations led to worse performance than on Weierstrass curves.

In this talk I will report on recent work with Arene, Naehrig, and Ritzenthaler in which we developed a geometric interpretation of the group law on twisted Edwards curves and derived explicit formulas for pairing computations that are competitive with those on Weierstrass curves. Correctnes of the fomulas was proved using the computer algebra system sage.

Pairings have found a lot of applications in cryptography and the speed of executing the protocols is directly linked to the speed of the pairing computation.

Keywords: Pairing, Miller function, explicit formulas, Edwards curves

Joint work of: Arene, Christof; Lange, Tanja; Naehrig, Michael; Ritzenthaler, Christof

Full Paper:
http://eprint.iacr.org/2009/155

Density of Ideal Lattices

Richard Lindner (TU Darmstadt, DE)

The security of many *efficient* cryptographic constructions, e.g. collision-resistant hash functions, digital signatures, and identification schemes, has been proven assuming the hardness of *worst-case* computational problems in ideal lattices. These lattices correspond to ideals in the ring of integers of some fixed number field K.

In this paper we show that the density of n-dimensional ideal lattices with determinant $\leq b$ among all lattices under the same bound is in $O(b^{1-n})$. So for lattices of dimension > 1 with bounded determinant, the subclass of ideal lattices is always vanishingly small.

Keywords: Post-quantum cryptography, provable security, ideal lattices

Joint work of: Buchmann, Johannes; Lindner, Richard

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2009/2125

Proving BSD for Small Elliptic Curves

Robert L. Miller (University of Washington, US)

Given an elliptic curve of rank 0 or 1, it is known that the order of the Shafarevich-Tate group (Sha) conjectured by Birch and Swinnerton-Dyer is an (easily computable) rational number. Work of Kolyvagin shows that the order of Sha is finite in these cases, and the true order of Sha can usually be computed.

For example, it is now known that if the conductor of a rank 0 or 1 curve is less than 1000, then the BSD conjectural formula holds for that curve. Examples will be given illustrating this process, after the necessary theory has been developed.

Keywords: BSD, Birch and Swinnerton-Dyer, elliptic curve, Shafarevich-Tate group

An algorithm to compute relative cubic fields

Anna Morra (Université Bordeaux, FR)

A result of Taniguchi generalizes the parametrization for cubic rings over Q (Levi / Delone -Faddeev / Davenport-Heilbronn) to cubic algebras over O_K for any number field K. We make this parametrization explicit using Dedekind criterion to test the maximality of an order in an extension of number fields, and we construct a notion of reduction using fundamental domains of the hyperbolic space H_3 under the action of linear groups. We obtain an algorithm, which uses in particular floating point computations and an "approximated" reduction for convenience and speed reasons, and we prove that the result is still exact, thanks to a theorem by Mahler.

Keywords: Cubic extensions, discriminant counting, Taniguchi parametrization, Julia reduction

On Imaginary Quadratic Quantum Public Key Cryptosystems

Ken Nakamula (Tokyo Metropolitan University, JP)

A general concept of Quantum Public Key Cryptosystem (QPKC), together with a concrete scheme OTU2000, was proposed in Crypto 2000.

The scheme requires quantum computer (QC) only in the step of generating public keys from private keys. We report our implemention of OTU2000 over imaginary quadratic fields. There are some practical problems even in the step of generating private keys without QC. We propose a practical algorithm of generating private keys. We next give a scheme to increase the density or the pseuod-density of generated subset-sum problems. The security of this scheme is, however, not yet clear. We also discuss an idea of generating public keys without QC. Although QPKC or OTU2000 is designed to use QC, it may be possoble to use it by classical computer alone.

Keywords: Quantum Public Key Cryptosystem, OTU2000, imaginary quadratic field

Joint work of: Nakamula, Ken; Nishimoto, Keiichiro

Zero-free regions for the derivatives of the Riemann Zeta Function

Sebastian Pauli (The University of North Carolina - Greensboro, US)

We investigate the zeros of derivatives of the Riemann zeta function $\zeta(\sigma + it)$ on the right of the line $\sigma = 1$ on the complex plane. We find previously unknown zero-free region depending only on σ and the degree of the derivative These zero-free regions are separated by narrow strips. Numerical evaluation of derivatives with high degree shows that these strips indeed contain zeros. Therefore, one cannot expect to extend the zero-free regions such that they connect to each other.

Keywords: Riemann zeta function, zeros of derivatives

Joint work of: Binder, Thomas; Pauli, Sebastian; Saidak, Filip

Lattice-based Blind Signatures

Markus Rueckert (TU Darmstadt, DE)

Motivated by the need to have secure blind signatures even in the presence of quantum computers, we present two efficient blind signature schemes based on hard worst-case lattice problems. Both schemes are provably secure in the random oracle model and unconditionally blind. The first scheme is based on preimage samplable functions that were introduced at STOC 2008 by Gentry, Peikert, and Vaikuntanathan. The scheme is stateful and runs in 3 moves. The second scheme builds upon the PKC 2008 identification scheme of Lyubashevsky. It is stateless, has 4 moves, and its security is based on the hardness of worst-case problems in ideal lattices.

Keywords: Blind signatures, post-quantum, lattices, privacy

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2009/2127

Full Paper:
http://eprint.iacr.org/2008/322

www.latticechallenge.org

Markus Rueckert (TU Darmstadt, DE)

Building upon a famous result due to Ajtai, we propose a sequence of lattice bases with growing dimension, which can be expected to be hard instances of the shortest vector problem (SVP) and which can therefore be used to benchmark lattice reduction algorithms.

The SVP is the basis of security for potentially post-quantum cryptosystems.

We use our sequence of lattice bases to create a challenge, which may be helpful in determining appropriate parameters for these schemes.

Keywords: Lattice reduction, lattice-based cryptography, challenge

Joint work of: Buchmann, Johannes; Lindner, Richard; Rückert, Markus; Schneider, Michael

Full Paper:
http://www.springerlink.com/content/036rkv616452w106/

See also: J. Buchmann and J. Ding (Eds.): PQCrypto 2008, LNCS 5299, pp. 79-94, 2008. (c) Springer-Verlag Berlin Heidelberg 2008

Construction of All Cubic Function Fields of Fixed, Even Degree Discriminant

Renate Scheidler (University of Calgary, CA)

For any odd prime power $q \equiv -1 \pmod 3$ and any squarefree polynomial $D \in \mathbb{F}_q[t]$ of even degree, we present an algorithm for generating all cubic function fields of discriminant D. In the case where the leading coefficient of D is not a square in $\mathbb{F}_q$, i.e. D is the discriminant of an unusual hyperelliptic function field, this method makes use of the infrastructure of the associated dual real hyperelliptic function field of discriminant $-3D$. This method was first proposed by D. Shanks for cubic number fields in an unpublished manuscript from the 1970s.

Keywords: Cubic function field, hyperelliptic function field, discriminant, signature, quadratic generator, reduced ideal

Probabilistic analysis of LLL-reduced bases

Michael Schneider (TU Darmstadt, DE)

LLL reduction, originally founded in 1982 to factor certain polynomials, is a useful tool in public key cryptanalysis. The search for short lattice vectors helps determining the practical hardness of lattice problems, which are supposed to be secure against quantum computer attacks.

It is a fact that in practice, the LLL algorithm finds much shorter vectors than its theoretic analysis guarantees. Therefore one can see that the guaranteed worst case bounds are not helpful for practical purposes. We use a probabilistic approach to give an estimate for the length of the shortest vector in an LLL-reduced bases that is tighter than the worst case bounds.

Keywords: Lattice reduction, LLL algorithm

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2009/2126

Constructing genus-2 curves and Jacobians of given order

Peter Stevenhagen (Universiteit Leiden, NL)

It was shown in the talk that one may efficiently construct, upon input of a number N together with its factorization, a genus-2 curve C over a finite field F having exactly N points defined over F.

Although the run time analysis is only heuristic, the numerical examples $N = 10^2009$ and $N = 10^{2009} + 2929$ (prime) were treated explicitly to illustrate the power of the method.

It constructs the curve C from its Jacobian J, which is isogenous to a product of elliptic curves that may be constructed using CM-methods in well-chosen small number fields.

In addition, we show that no efficient CM-algorithm exists to solve the related problem of constructing a genus-2 curve C over a finite field F for which the Jacobian J has a prescribed number N of F-rational points.

This is joint work with Everett Howe (CCR) and Kristin Lauter (Microsoft Research).

Rational Points on Curves of Genus 2: Experiments and Speculations

Michael Stoll (Universität Bayreuth, DE)

We present results of computations providing statistics on rational points on (small) curves of genus 2 and use them to present several conjectures. Some of these conjectures are based on heuristic considerations, others are based on our experimental results.

Keywords: Rational points, genus 2

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2009/2124

Theta functions, class units and some applications

Osmanbey Uzunkol (TU Berlin, DE)

Instead of taking a random elliptic curve over a finite field and computing the cardinality of rational points, it is possible to construct special elliptic curves with a known number of rational points with the theory of complex multiplication. To do this, we need to compute the minimal polynomial of $j-$ invariants evaluated at $\tau \in K \cap \mathbb{H}$, where K is an imaginary quadratic number field. There are other functions, the so-called class invariants, whose values at τ generate the same field and have minimal polynomials having smaller heights than the corresponding minimal polynomials of the singular values of the $j-$invariant.

We are going to introduce the classical class invariants of Weber as quotients of so-called Thetanullwerte, which enables us to compute these invariants more efficiently than as quotients of values of the Dedekind $\eta-$function.

We show secondly how to compute the unit group of suitable ring class fields by means of proving the fact that most of the invariants introduced by Weber are actually units in the corresponding ring class field by a theorem of Deuring.

Keywords: Complex multiplication, theta functions

The SCIEnce project

Osmanbey Uzunkol (TU Berlin, DE)

The SCIEnce project (Symbolic Computation Infrastructure for Europe) brings together the developers of four powerful symbolic computation software packages (GAP, KANT, Maple and MuPAD) and a major symbolic computation research institute (RISC-Linz) supported by research groups expert in essential underpinning technologies, to unite the European community of researchers in, and users of, symbolic computation.

We are going to introduce the SCIence project and its goals as well as the SCSCP (Symbolic Computation Software Composibility Protocol), based on OpenMath, by which a computer algebra system (CAS) may offer services and a client may employ them.

Keywords: Computer algebra systems, symbolic computation

Standard models of finite fields: the definition

Bart de Smit (Leiden University, NL)

We present a definition of an explicit model of the field of q elements that has good algorithmic properties.

Keywords: Finite fields

Joint work of: de Smit, Bart; Lenstra, Hendrik