Algorithms and Number Theory

13.05.2001-18.05.2001

organized by

J. Buhler (Berkeley),
H. Niederreiter (Singapore),
M.E. Pohst (Berlin)

Preface

This seminar on number-theoretical algorithms and their applications was the fourth on this topic at Dagstuhl over the last 10 years. This year 45 people from 14 countries participated.

One of the major goals of these 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 this year almost a third of the talks were on algebraic curves, most with an eye to applications in cryptography. The use of elliptic curves in cryptography seems to be well understood by now, and the focus is on speeding up the algorithms, whereas the research on the use of hyperelliptic curves is more focused on developing the mathematical foundations of the field.

Many other talks focused on more classical topics of algebraic number theory, such as finding divisor class groups of function fields, finding galois groups, and investigating class groups and their heuristics.

The remaining talks covered a wide variety of problems in algorithmic number theory, including hardware implementations of arithmetic over fields of characteristic 2, a parallel sorting algorithm with applications to integer factorization, find solutions to diophantine equations, and factoring polynomials in various domains.

The variety of topics was stimulating to the audience (though it did make the organizers' task of grouping the talks more difficult!). The reaction of the participants was quite 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.

Contents

1 LLL-type Reduction of Lattice Bases in $O(n^3 \log_2 n)$ Arithmetic Steps on Bounded Integers.

Henrik Koy, Claus Peter Schnorr

We present a variant of LLL-reduction of lattice bases in the sense of LENSTRA, LENSTRA, LOVÁSZ. We organize LLL-reduction in segments of size k. Local LLL-reduction of segments is done using local coordinates of dimension k.

We introduce *segment* LLL-*reduced bases*, a variant of LLL-reduced bases achieving a slightly weaker notion of reducedness, but speeding up the reduction time of lattices of dimension n by a factor n. We also introduce a variant of LLL-reduction using *iterated segments*. The resulting reduction algorithm runs in $O(n^3 \log_2 n)$ arithmetic steps for integer lattices of dimension n with basis vectors of length 2^n.

2 Saturation of Mordell-Weil groups

John Cremona

Given a subgroup B of a finitely-generated abelian group A, the saturation $\overline{B}$ of B is defined to be the largest subgroup of A containing B with finite index. We considered the case where $A = E(K)$, the Mordell-Weil group of an elliptic curve E defined over a number field K, and where B is the subgroup generated by a given set of K-rational points. This situation occurs, for example, when computing $E(K)$ by 2-descent, where we normally obtain a set of points which generate a subgroup of $E(K)$ of finite (odd) index, and wish to extend to a basis for the full group $E(K)$.

The problem divides into two: first to determine an upper bound n_0 for the index $n = [\overline{B} : B]$, and second to decide, for each prime p less than n_0, whether or not B is p-saturated (in the obvious sense). The first problem, which was not discussed in detail, uses estimates from the geometry of numbers. For the second problem, the method consists in constructing many group homomorphisms $E(K) \to \mathbb{F}_p$, since B is p-saturated if and only if

there exists a map $f : E(K) \to \mathbb{F}_p^N$ which is injective on B/pB. Two methods were described, both using auxilary primes q and such that $p \mid \#E(\mathbb{F}_q)$. Both methods have been implemented for $K = \mathbb{Q}$. The first method, due to Siksek, is to map to a subgroup of order p in $E(\mathbb{F}_q)$ and hence (via an elliptic curve discrete logarithm) to $\mathbb{F}_p$. This has certain drawbacks which were described. A newer and more elegant method using a map related to the Tate-Lichtenbaum pairing was then described, where the map is to $\mathbb{F}_q^*/(\mathbb{F}_q^*)^p$ for $q \equiv 1 \pmod{p}$, and hence (via a discrete logarithm in $\mathbb{F}_q^*$) to $\mathbb{F}_p$. The resulting algorithm appears to work well in practice, despite the restriction that only primes $q \equiv 1 \pmod{p}$ can be used. In answer to a question from the audience, it was (later) confirmed that the use of sufficiently many primes q will always be sufficient to prove that a p-saturated subgroup of $E(K)$ is indeed p-saturated.

3 Some New Results on Pseudoprimality Testing

Siguna Müller

Although the Miller-Rabin test is very fast in practice, there exist composite integers n for which this test fails for 1/4 of all bases coprime to n. In 1998 Grantham developed a probable prime test with failure probability of only 1/7710 and asymptotic running time three times that of the Miller-Rabin test. For the case that $n \equiv 1 \bmod 4$, recently a test with failure rate of 1/8190 and comparable running time as for the Grantham test was established by the author. Already in 1980, Pomerance, Baillie, Selfridge, and Wagstaff developed a very efficient probable prime test for which no composite number is known that passes it. Based on their ideas we propose a probable prime test which always has running time at most three times the time as for the Miller-Rabin test. A composite integer $n \equiv 3 \bmod 4$ will pass our test with probability less than 1/131040.

4 Addition Chains and the Scholz Conjecture

Ken Nakamula (joint work with Hatem M. Bahig)

For an integer $n > 0$, an *addition chain* of *length* r is a sequence $1 = a_0 < a_1 < \cdots < a_r = n$ such that

$$a_i = a_j + a_k \quad \text{with} \quad 0 \le k \le j < i \quad \text{for} \quad 0 < i \le r.$$

The step a_i is called *star* if $j = i - 1$. An ℓ°-*chain* is an addition chain such that some of the $a_0, \ldots, a_r$ are underlined and, for $0 < i \le r$, a_j is the largest underlined element less than a_i. We denote the minimum length of all addition chains or all ℓ°-chains for n by $\ell(n)$ or $\ell^\circ(n)$ respectively. In 1937, Arnold Schloz conjectured that, for all $n \ge 1$, we have

$$\ell(2^n - 1) \le n + \ell(n) - 1.$$

Clearly $\ell(n) \le \ell^\circ(n)$. It is not known whether or not

$$\ell(n) = \ell^\circ(n)$$

in all cases. If this is true, then the Scholz conjecture is also true. Let $\nu(n)$ be the number of 1's in the binary representation of n
Proving some properties of *nonstar* steps in addition chains, we obtain

Theorem 1. *Assume*

$$5 \le \nu(n) \le 8 \quad \textit{and} \quad \ell(n) = \lfloor \log_2 n \rfloor + 3.$$

If there is a shortest addition chain for n, then there is a shortest ℓ°-chain of the same length.

As a corollary, we have

Theorem 2. *Assume either*

$$\nu(n) \le 5$$

or

$$6 \le \nu(n) \le 8 \quad \textit{and} \quad \ell(n) = \lfloor \log_2 n \rfloor + 3.$$

Then $\ell^\circ(n) = \ell(n)$, and hence the Scholz conjecture is true.

5 An Introduction to Schimmler sorting

D. Bernstein

One can sort n^2 numbers on an $n \times n$ processor mesh in $O(n)$ parallel compare-exchange steps. Schimmler's algorithm is a very simple algorithm that uses $8n - 8$ steps. I explained (1) odd-even transposition sorting; (2) Schimmler sorting; (3) the relevance of these results to integer factorization.

6 The "diagonal case" of Nagell's equation $\frac{x^p-1}{x-1} = y^p$

P. Mihailescu

We investigate an approach to the diagonal case of Nagell's equation, which is based upon Abel series expansions of algebraic numbers generated by applying Stickelberger ideal elements to ideals which stem from presumed solutions to the diagonal case.

7 Power integral bases in infinite parametric families of simplest number fields

István Gaál (Debrecen)

To find generators α of power integral bases $\{1, \alpha, \dots, \alpha^{n-1}\}$ of number fields K of degree n requires usually hard computations involving reduction methods and enumeration algorithms.
It is especially interesting to consider power integral bases in infinite parametric families of number fields and to try to describe their generators in a

parametric form. We consider this problem in the so called simplest parametric families of fields.
Power integral bases in the simplest cubic, simplest quartic and simplest quintic number fields were considered formerly. The main topic of the talk is to consider power integral bases in the simplest sextic fields. Denote by O the order of the simplest sextic fields composed by the main order of their cubic subfield and the main order of their quadratic subfield. It was shown by I.Gaál, P.Olajos and M.Pohst that the indices of all elements of O are divisible by a constant, hence O has no power integral bases. This statement is the consequence of a more general theorem.

8 Algorithms for divisor class groups of global function fields

Florian Heß

Algorithms for divisor class groups of global function fields Florian Heß, University of Bristol
Given a global function field F/k we consider two main tasks: 1. Compute the structure of the divisor class group $Cl \cong \mathbb{Z} \times \mathbb{Z}/c_1\mathbb{Z} \times \cdot \times \mathbb{Z}/c_{2g}\mathbb{Z}$ and 2. Find a method to compute images and preimages under the map $Cl \to \mathbb{Z}\times\mathbb{Z}/c_1\mathbb{Z}\times\cdot\times\mathbb{Z}/c_{2g}\mathbb{Z}$. Both tasks can be dealt with by an index calculus style method which essentially computes S-units for a suitably chosen finite set S of places. The expected running time of the method is subexponential of the form $\exp(c\sqrt{g\log(g)})$ ($c > 0$, g the genus) for fixed finite field size, a fixed extension degree $[F : k(x)]$ and under a certain smoothness assumption. The algorithm extensively uses a new (ideal theoretical) method for computing Riemann-Roch spaces of divisors, which is useful in many other contexts as well.

9 On Minimal Discriminants

Jürgen Klüners

In this talk we present a database for number fields up to degree 15. The database contains about 100000 fields. It includes at least one polynomial f with $\mathrm{Gal}(f) = G$ for every transitive group G up to degree 15. In fact, such polynomials are given for most of the combinations of groups and possible signatures. Here we restrict ourselves to the problem of computing minimal discriminants for fields with given Galois group and signature. It is well known that up to degree 6, complete results can be obtained using techniques based on the geometry of numbers. The same techniques were successfully applied to complete the degree 7 case.
Cohen, Diaz y Diaz, and Olivier computed all minimal discriminants for imprimitive octic extensions containing a quartic subfield. Their approach uses class field theory to generate relative quadratic extensions. Here we generalize this approach to some meta-abelian groups. Especially Frobenius groups are suited for our new method. We compute all minimas for octic extensions containing only a quartic subfield. Furthermore we determine the minimal discriminants for two primitive groups in degree 8. We give the minimas for all Frobenius groups in prime degree up to degree 13.
This is a joint work with Claus Fieker and Gunter Malle

10 The Index Calculus Method using non-smooth polynomials

Theo Garefalakis and Daniel Panario

We study a generalized version of the index calculus method for the discrete logarithm problem in $\mathbb{F}_q$, when $q = p^n$, p is a small prime and $n \to \infty$. The database consists of the logarithms of all irreducible polynomials of degree between given bounds; the original version of the algorithm uses lower bound equal to one. We show theoretically that the algorithm has the same asymptotic running time as the original version. The analysis shows that the

best upper limit for the interval coincides with the one for the original version. The lower limit for the interval remains a free variable of the process. We provide experimental results that indicate practical values for that bound. We also give heuristic arguments for the running time of the Waterloo variant and of the Coppersmith method with our generalized database.

11 NFS polynomial selection algoritms for discrete logs computation

Igor Semaev

The number field sieve (NFS) is a method for factoring integers and discrete logs computation. Let N be an integer number to be factored or $N = p$ be a prime number in a prime finite field of order p. At first the prerequisite of the NFS was a congruence

$$f(m) \equiv 0 \pmod{N},$$

where $f(X)$ is an irreducible polynomial in $\mathbb{Z}[X]$ and $m \in \mathbb{Z}$. The main parameter of the method is $n = \deg f(X)$. The other ones such as m and the coefficients of $f(X)$ may be bounded by $N^{\frac{1}{n+1}}$ in absolute value. It is easy to find such congruence for any given N and n. We have here the two polynomials $f(X)$ and $X - m$ having the common root m modulo N.
One can use nonlinear polynomials $f(X), g(X)$ with a common root modulo N. We have the following congruence

$$\mathrm{Res}\,(f(X), g(X)) \equiv 0 \pmod{N}$$

for these polynomials. Using nonlinear poynomials increases the probability of finding relations for factoring and in the discrete logs computation with the NFS.
Generally it is very difficult to find nonlinear polynomials $f(X)$, $g(X)$ with small coefficients such that the congruence for their resultant holds. We see

$$\mathrm{Res}\,(f(X), g(X)) = O(|f|^{n_1}|g|^{n_2})$$

for fixed $n_1 = \deg f, n_2 = \deg g$, where

$$|f| = |a_0 X^{n_1} + a_1 X^{n_1 - 1} + \cdots + a_{n_1}| = \max_i |a_i|$$

and

$$|g| = |b_0 X^{n_2} + b_1 X^{n_2-1} + \cdots + b_{n_2}| = \max_j |b_j|.$$

We consider the the following problem: Given N (or $N = p$), n_1 and n_2, find $f(X)$ of degree n_1 and $g(X)$ of degree n_2 such that

$$|f| \approx |g| \approx N^{\frac{1}{n_1+n_2}}$$

and

$$\mathrm{Res}\,(f(X), g(X)) \equiv 0 \mod N,$$

but

$$\mathrm{Res}\,(f(X), g(X)) \neq 0.$$

For $n_1 = n_2 = 2$ and any integer N this problem was solved by P. Montgomery. The main result of this talk is a solution of this problem for $n_1 = 2$ and any natural n_2. But this holds only for prime numbers p.

12 Average time analysis of Hensel lifting

Shuhong Gao

We present an average time analysis of a Hensel lifting based factorisation algorithm for bivariate polynomials over finite fields. It is shown that the average running time is almost linear in the input size. This explains why the Hensel lifting technique is fast in practice for most polynomials.

13 New computations concerning the Cohen-Lenstra class number heuristics

Herman te Riele (joint work, in progress, with Hugh C. Williams)

A fast algorithm is presented to compute the class number h of the real quadratic field $K = Q(\sqrt{p})$, where p is a prime $\equiv 1 \bmod 4$. This algorithm is based on the infrastructure idea of Shanks to determine the regulator of K and then it uses the Extended Riemann Hypothesis to rapidly estimate $L(1, \chi_p)$ and compute an accurate estimate $\tilde{h}$ of h with help of the analytic class number formula. In most cases it is possible next to prove that $\tilde{h} = h$, with the use of an improvement by Williams of an upper bound of Bach of the error in the estimate of $L(1, \chi_p)$.
Preliminary experiments are reported in which the primes $\equiv 1 \bmod 4$ are counted with $h = 1$ and $h = 3$, in twenty consecutive intervals of length 10^9, starting with the interval $[1, 10^9]$. The computed fractions of primes with $h = 1$ and $h = 3$ are 0.758820 and 0.122495, respectively, and these agree reasonably well with the Cohen-Lenstra heuristics which predict fractions 0.754458 and 0.125743, respectively.

14 C_4-extensions of number fields

Henri Cohen

In recent years, there has been considerable progress in methods for finding asymptotic estimates for the number $N_{K,n}(G, X)$ of extensions of degree n of a number field K whose Galois group of the normal closure is isomorphic to G and whose absolute discriminant is bounded by X. In particular, for $K = \mathbb{Q}$ such a formula is known for all abelian groups G, for $G = D_4$ the dihedral group of order 8, for $G = A_4$ the alternating group, and conjecturally for $G = S_4$.
For an arbitrary number field K the situation is much less satisfactory. In a difficult 50-page (submitted) paper, the author together with F. Diaz y Diaz

and M. Olivier solve the problem for $G = C_\ell$, the cyclic group of prime order ℓ. Even the case $\ell = 2$, which was known before, is not trivial.
Although it would seem tempting to use class field theory for these problems, it is a fact that only Kummer theory can give satisfying answers, in particular by using a well-known theorem of Hecke giving the relative discriminant of a cyclic Kummer extension of prime degree ℓ.
It would be nice to have an analogous theorem for higher powers of ℓ. The first problem to be solved is to find an explicit $\mathfrak{p}$-integral basis for a Kummer extension of prime degree ℓ. This is in principle already done by Hecke, but the result (too long to be given here) is quite amusing and involves both the solution of the Hecke congruences (not surprising), but also all the "derivatives" of a given polynomial in the primitive element.
In the special case of C_4-extensions, hence with $\ell = 2$, we can then go on and find completely explicitly the generalization of Hecke's theorem. It is quite plausible that this can be done in general, although I do not yet know the details. In the C_4-case, what is also quite amusing is that the result involves not only solving Hecke congruences of the type $\beta^2 \equiv \alpha \pmod{\mathfrak{p}^k}$, but also $x^2 \equiv \gamma \pmod{\mathfrak{p}^k}$ where

$$\gamma = \frac{i}{\beta}\frac{\alpha - \beta^2}{2} - \beta \,. \pmod{\mathfrak{p}^k}$$

The next step is to use this to compute $N_{K,4}(C_4, X)$ when $i \in K$, but I have not done that yet.

15 On the Computation of Galois Groups

K. Geißler

Methods for computing Galois groups over the rationals are well known. We focus on the method of Stauduhar which in particular allows us to compute efficiently Galois Groups of higher degrees. In order to extend Stauduhar's algorithm to other coefficient rings, such as algebraic number fields F or rational function fields over Q and finite fields F_q two problems arise:

(i) The representations of the roots $\alpha_1, \ldots, \alpha_n$ of the polynomial f, whose Galois group we would like to calculate.

(ii) How to perform the inclusion test; in other words how to decide whether a combination of the α_i is an element of the maximal order of $F, Q(x)$ or $F_q(x)$.

We give possible solutions for these problems for the above fields. Moreover we describe our implementation and present some experimental results for irreducible polynomials over F and $Q(x)$ up to degree 23.

16 Correction factors for primitive root densities

Peter Stevenhagen

It follows from the work of Artin and Hooley that, under assumption of the generalized Riemann hypothesis, the density of the set of primes q for which a given rational number x is a primitive root modulo q can be written as an infinite product $\prod_p A_p$ of local factors times a somewhat complicated correction factor reflecting the fact that the quadratic field $\mathbf{Q}(\sqrt{x})$ is contained in certain cyclotomic fields. We show that correction factors of this nature also admit a description in terms of local contributions, and apply this to evaluate the densities for a number of generalizations of Artin's original primitive root problem.
This is joint work with Pieter Moree and Hendrik Lenstra.

17 Polynomial Factorization over Local Fields

David Ford, Sebastian Pauli and Xavier-François Roblot

The factorization algorithm of Ford, Pauli, and Roblot is included in Pari/GP 2.1.1. Comparisons with other systems, using examples known to be "difficult", show considerably better performance.

The new algorithm of Pauli has expected compexity

$$O\big(N^{3+\epsilon} v_{\mathfrak{p}}(\operatorname{disc}\Phi)^{1+\epsilon} \log^{1+\epsilon} p^k + N^{2+\epsilon} v_{\mathfrak{p}}(\operatorname{disc}\Phi)^{2+\epsilon} \log^{1+\epsilon} p^k\big),$$

an improvement of $O\big(N(N + v_{\mathfrak{p}}(\operatorname{disc}\Phi))\big)$ over previously published results. Two examples of the operation of Pauli's algorithm are given in detail.

18 On Minimal Expansions in Redundant Number Systems: Algorithms, Quantitative Analysis, and Extensions

Clemens Heuberger (partly joint work with Helmut Prodinger)

We study redundant q-ary digit expansions

$$n = \sum_{j=0}^{l} \varepsilon_j q^j$$

with arbitrary integer digits $\varepsilon_j \in \mathbb{Z}$ for positive integers n and $q \geq 2$. We call such an expansion minimal if $1 + l + \sum_{j=0}^{l} |\varepsilon_j|$ is minimum. The binary case $q = 2$ (partly with other cost functions) has been studied by several authors, motivated by applications from cryptography and coding theory.
There is not a unique minimal expansion. We define the notion of a reduced expansion of n in base q. For all n and bases q, there is a unique reduced expansion, and this expansion minimizes the costs under investigation.
The syntactical properties of such expansions are characterized. This enables us to determine the jth digit of a minimal expansion from the knowledge of the jth and $(j + 1)$th digits of the "standard" q-ary expansion, i. e., the unique expansion with digits $0, \dots, q - 1$. This leads to a straightforward algorithm for the calculation of minimal expansions. Additionally, we give an explicit formula for the jth digit of a minimal expansion without having to calculate the other digits. This formula makes it possible to calculate the expected costs of minimal expansions.
Finally we deal with the question whether such results can be generalized to other number systems, for instance canonical number systems in an algebraic

number field. We give a negative answer for the case of the ring of Gaussian integers and bases $-a+i$.

References:

1. C. Heuberger and H. Prodinger, On Minimal Expansions in Redundant Number Systems: Algorithms and Quantitative Analysis, to appear in Computing.

2. C. Heuberger, Minimal Redundant Digit Expansions in the Gaussian Integers, to appear in J. Theor. Nombres Bordeaux.

19 Two - Descent

F. Lemmermeyer

Let $E : y^2 = x(x^2+ax+b)$ be an elliptic curve defined over $\mathbb{Q}$; for computing the rank of its Mordell-Weil group it is sufficient to decide whether certain curves $T : N^2 = rM^4 + sM^2e^2 + te^4$ (with given $r, s, t \in \mathbb{Z}$) have rational points. Using a trick due to Lagrange it can be shown that if $x^2 = rm^2 + sme + te^2$ has a rational point, then the curves T can be factored over $\mathbb{Q}$, and studying these factors over the p-adic completions of $\mathbb{Q}$ often allow us to conclude that T does not have a rational point.

20 Number-theoretic Graphs?

Amin Shokrollahi

Often in traditional coding theory one proves properties of codes using algebraic or combinatorial tools, and then tries to find decoding algorithms that decode as many errors as predicted by the theory. In contrast, low-density parity-check codes come equipped with efficient algorithms. Here,

one tries to identify those codes in the class on which the algorithm performs particularly well, i.e., for which the algorithm can correct lots of errors.
In this talk I will give a short introduction into these codes. As it turns out, for decoding erasures, one needs an expansion property of the bipartite graph underlying the codes. I will give some examples of number-theoretic graphs that have expansion for very small sets, and will pose the problem of designing other number-theoretic graphs for which larger sets expand.

21 Jacobians of Elliptic Curves with Complex Multiplication

A. Weng

We present a generalization of the well-known complex multiplication method for elliptic curves due to Atkin and Morain to hyperelliptic curves. This algorithm constructs a curve whose Jacobian has complex multiplication by the maximal order in a given CM-field.
We give examples for genus 2 and 3.

22 Factoring $N = pq^2$ with the Elliptic Curve Method

Edlyn Teske

Various cryptosystems have been proposed whose security relies on the difficulty of factoring integers of the special form $N = pq^2$. To factor integers of that form, Peralta and Okamoto introduced a variation of Lenstra's Elliptic Curve Method (ECM) of factorization, which is based on the fact that the Jacobi symbols $\left(\frac{a}{N}\right)$ and $\left(\frac{a}{p}\right)$ agree for all integers a, $\gcd(a, q) = 1$. The authors report that this variation is by a factor of about $\log p$ faster than the

Basic Variant of ECM.
We report on an implementation and extensive experiments with that variation, which have been conducted in order to determine the speed-up compared with an improved variant of ECM called the Standard Continuation. Our results indicate that the Standard Continuation is expected to factor $N = pq^2$ about twice as fast as the Jacobi symbol variant. Thus, integers of the form $N = pq^2$ ($p \approx q$) still seem to be no easier to factor with ECM than numbers of the form $N = pq$ ($p \approx q$).
This is joint work with Peter Ebinger from Karlsruhe University, Germany.

23 Algorithms for the Hardware Implementation of $\mathbb{F}_{2^{12}}$ and $\mathbb{F}_{2^{15}}$ Arithmetic using Splitting Fields

Erich Wehrhahn

The motivation for the implementation of $\mathbb{F}_{2^{12}}$ and $\mathbb{F}_{2^{15}}$ is given by the need to implement error correcting codes with data blocks of 32640 bits. The candidates for the codes are Reed-Solomon in $\mathbb{F}_{2^{12}}$ (operands $+^*/$) and BCH in $\mathbb{F}_{2^{15}}$ (operands $+^*$) . The implementation uses composite fields that have AND and XOR basic hardware components in $\mathbb{F}_2$ and a first extension either to $\mathbb{F}_{2^3}$ or $\mathbb{F}_{2^4}$ based on a primitive polynomial. The second extension to the $\mathbb{F}_{2^{12}}$ or $\mathbb{F}_{2^{15}}$ fields is performed with a rational function such that the composite field is defined also by a primitive polynomial. The results of the different implementations are compared for the gate count used for the arithmetic operations. The open problems are: the efficient root determination of polynomials and the recursive implementation of the Massey-Berlekamp Algorithm.

24 Woltman's conjecture on the Lucas-Lehmer test

H. W. Lenstra, Jr.

Let p be an integer, $p > 1$, and put $q = 2^p - 1$. Let $s \in \mathbf{Z}/q\mathbf{Z}$, and define the sequence $(s_i)_{i=1}^{\infty}$ of elements of $\mathbf{Z}/q\mathbf{Z}$ by $s_1 = s$, $s_{i+1} = s_i^2 - 2$. Then one has $s_{p-1} = 0$ if and only if the following three conditions are satisfied: q is prime; the Jacobi symbol $\left(\frac{s-2}{q}\right)$ equals 1; and $\left(\frac{s+2}{q}\right) = -1$. This is the Lucas-Lehmer primality test. For all odd values of p, the Jacobi symbol conditions are satisfied if s is one of 4, 10, and $\frac{2}{3}$ (modulo q). Suppose now that $p > 2$, and that $s_{p-1} = 0$. Then q is prime and p is odd, and $s_{p-2}^2 = 2 = (2^{(p+1)/2})^2$ (in $\mathbf{Z}/q\mathbf{Z}$), so one has $s_{p-2} = \epsilon \cdot 2^{(p+1)/2}$ for a unique sign $\epsilon = \epsilon(s,p) \in \{\pm 1\}$. George Woltman observed in 1996 that for 29 of the 30 values of p that are at most 216091 one has $\epsilon(4,p) \cdot \epsilon(10,p) = -1$ or 1 according as $p \equiv 1$, 3 mod 8 or $p \equiv 5$, 7 mod 8, the sole exception being $p = 5$. Similarly, one can observe that one has $\epsilon(\frac{2}{3},p) \equiv p \bmod 4$ for every value of p that one tries except $p = 5$. In the lecture it was shown that these observations hold in full generality for $p \neq 5$. The proof makes use of class field theory. It is taken from the Berkeley Ph.-D. thesis of S. Y. Gebre-Egziabher.

25 Independence of Rational Points on Hyperelliptic Curves

Michael Stoll

Consider the following question. Let $C/\mathbb{Q} : y^2 = f(x)$ be a hyperelliptic curve of genus $g \geq 2$, and let J denote its Jacobian. Map $C(\mathbb{Q}) \ni P \mapsto [2 \cdot P - (x)_\infty] \in J(\mathbb{Q})$. Given a subset $S \subset C(\mathbb{Q})$, to what extent are its elements independent in $J(\mathbb{Q})$? More precisely: Can we bound $r(S)$, the rank of the subgroup generated by the images in $J(\mathbb{Q})$ of the elements of S, from below in terms of the size of S?
In general, nothing is known about this question. However, when we restrict to quadratic twists of a given curve, there is the following result, which may

be extracted from a paper by Joe Silverman (J. London Math. Soc., 1993).

Theorem. *There is a constant $\gamma(C)$ such that for all quadratic twists C_d of C and all subsets $S \subset C_d(\mathbb{Q})$, we have*

$$r(S) \geq \log \#S - \gamma(C)\,.$$

This gives us some information when the set S is very large. By contrast, we prove the following. Note that we can eliminate trivial relations by requiring S and S' to be disjoint, where $P \mapsto P'$ is the hyperelliptic involution.

Theorem. *For all but finitely many quadratic twists C_d of C, we have*

$$r(S) = \#S$$

for all subsets $S \subset C_d(\mathbb{Q})$ such that $S \cap S' = \emptyset$ and $\#S \leq g$. If we suppose the twisting factor d to be a squarefree integer, then the exceptions all have d divisible only by primes not larger than $2\#S+1$ or by primes of bad reduction for C.

Clearly, this result is best possible, apart from the bound on the size of the set S. This restriction is inherent in the method of Chabauty-Coleman, which we use for the proof.

26 Computing the Modular Degree of an Elliptic Curve

M. Watkins

Let E be a rational elliptic curve of conductor N and $X_0(N)$ be the modular curve that classifies cyclic N-isogenies. By the work of Wiles and others, it is known that there is a surjective morphism from $X_0(N)$ onto E. As both $X_0(N)$ and E can be viewed as Riemann surfaces (or algebraic curves), this mapping has an associated degree, which is the modular degree. There is a known "class-number" formula that relates the modular degree to a special value of some L-function, in this case, that of the symmetric square of the elliptic curve. This allows us to compute the modular degree via computation of the special L-value to sufficiently high precision, a task for which a

generic technique already exists. We report on data from over 50000 curves that we have considered, and comment on heuristics of Cohen-Lenstra type concerning how often a given odd prime should divide the modular degree.

27 Modular Curves of Positive Genus and Elliptic Curve Cryptosystems

Andreas Enge (joint work with Reinhard Schertz)

We present a class of functions on modular curves $X^0(N)$ whose values generate ring class fields of imaginary quadratic orders. This is used to develop a new algorithm for constructing elliptic curves over finite fields with known complex multiplication and thus with known group order. Applications of this algorithm are elliptic curve primality proving and the construction of secure elliptic curve cryptosystems. The difficulties arising when the genus of $X^0(N)$ is not zero are overcome by computing certain modular polynomials. Being a product of four η-functions, the proposed modular functions are a natural generalisation of the Schläfli functions examined by Weber and usually employed to construct CM-curves. Unlike the Schläfli functions, the values of the examined functions generate any ring class field of an imaginary quadratic order regardless of the congruences modulo powers of 2 and 3 satisfied by its discriminant. For discriminants to which both classes of functions apply, we compare their relative efficiency.

28 Visualising Ш[2] in Abelian surfaces over Number Fields

Nils Bruin

We consider an elliptic curve

$$E : y^2 = x^3 + a_2\,x^2 + a_4\,x + a_6$$

over a number field K. Its set of rational points $E(K)$ forms a finitely generated commutative group. We have that $E(K) \simeq \mathbb{Z}^r \times E(K)^{\mathrm{tor}}$, where $E(K)^{\mathrm{tor}} \subset E(K)$ is the finite subgroup of elements of finite order. This group is effectively and in practice usually easily determinable. In order to determine r, the *rank* of $E(K)$, it would be sufficient to determine the size of $E(K)/2E(K)$. From Galois-cohomology we obtain

$$0 \to E(K)/2E(K) \to H^1(K, E[2]) \to H^1(K, E)$$

The middle term, $H^1(K, E[2])$, classifies twists of $E \xrightarrow{2} E$, that is, unramified $E[2]$-covers $T \to E$ that are isomorphic to $E \to E$ over $\overline{K}$. The image of $E(K)/2E(K)$ corresponds to $T \in H^1(K, E[2])$ with $T \neq \emptyset$. An effectively determinable approximation of $E(K)/2E(K)$ is given by the *Selmer-group*

$$S^{(2)}(E/K) = \{T \in H^1(K, E[2]) : T(K_p) \neq \emptyset \text{ for all completions } K_p \text{ of } K\}.$$

The error in this approximation is defined to be the Tate-Shafarevich group

$$0 \to E(K)/2E(K) \to S^{(2)}(E/K) \to Ш(E/K)[2] \to 0.$$

It is represented by T that have points locally at all primes of K but not globally over K.
Given an elliptic curve E and a $T \in S^{(2)}(E/K)$ that we suspect to have a non-trivial image in $Ш(E/K)[2]$, we can do the following. We compute a value $d \in K$ so that $T(K(\sqrt{d})) \neq \emptyset$. We use that

$$\mathrm{rk}(E(K(\sqrt{d}))) = \mathrm{rk}(E(K)) + \mathrm{rk}(E^{(d)}(K)),$$

where

$$E^{(d)} : d\,(y')^2 = x^3 + a_2\,x^2 + a_4\,x + a_6.$$

We get an upper bound on $\mathrm{rk}(E(K(\sqrt{d})))$ by computing $S^{(2)}(E/K(\sqrt{d}))$. If we can get a sufficiently high lower bound on $\mathrm{rk}(E^{(d)}(K))$ (for instance, by

exhibiting sufficiently many independent points on $E^{(d)}(K)$), then we can show that the rank bound obtained from $S^{(2)}(E/K)$ is not sharp.
A rather striking example is given by

$$E : y^2 = x^3 - 22x^2 + 21x + 1.$$

We find $\#S^{(2)}(E/\mathbb{Q}) = 16$ and $\mathrm{rk}(E(\mathbb{Q})) > 2$. Furthermore, we get $\#S^{(2)}(E^{(2)}/\mathbb{Q}) = 16$ and $\mathrm{rk}(E^{(2)}(\mathbb{Q})) > 2$. However, we compute $\#S^{(2)}(E/\mathbb{Q}(\sqrt{2})) = 16$. Therefore, we find that $\#Ш(E/\mathbb{Q})[2] = \#Ш(E^{(2)}/\mathbb{Q})[2] = 4$.
We see that $E/\mathbb{Q}$ and $E^{(2)}/\mathbb{Q}$ mutually visualise $Ш[2]$ in the sense of Cremona-Mazur in the Weil-restriction $\Re_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(E)$.
We do not need to restrict to Abelian surfaces that are Weil-restrictions of elliptic curves. Note that $E : y^2 = F(x)$ is a double cover of $\mathbb{P}^1$ by $(x, y) \mapsto x$. Let

$$L : z^2 = d(x - a) \text{ and } C = L \times_{\mathbb{P}^1} E.$$

Then C is a curve of genus 2 given by $y^2 = F(z^2/d + a)$. Apart from E and L, the curve C also covers

$$E' : (y')^2 = d(x - a)F(x).$$

This implies that

$$\mathrm{rk}(\mathrm{Jac}_C(K)) = \mathrm{rk}(E(K)) + \mathrm{rk}(E'(K)).$$

We can bound the left hand side from above by determining the 2-Selmer group of Jac_C.
For instance, if we choose $a = 1$, $d = -1$ in the example above, we find $\mathrm{rk}(\mathrm{Jac}_C(\mathbb{Q})) \leq 5$ and $\mathrm{rk}(E'(\mathbb{Q})) = 3$. Again we find $\mathrm{rk}(E(\mathbb{Q})) = 2$ and $\#Ш(E/\mathbb{Q})[2] = 4$.
An advantage of the latter construction is that the two degrees of freedom (a and d) allow us solve for visualisation of two elements of $S^{(2)}(E/K)$ simultaneously. This helps because, conjecturally, $Ш[2]$ always has square order.