Tagungsbericht: 27/1999

Explicit Methods in Number Theory

4.7. - 10.7.1999

The conference was organized by H. Cohen (Talence), H. Lenstra (Berkeley, Leiden) and D. Zagier (Bonn, Utrecht). The goal was to present new methods and results on concrete aspects of number theory. In many cases this included computational and experimental work, but with the primary emphasis being on the implications for number theory rather than on the computaional methods used.

There were two "mini-series" of two 1-hour lectures each, one by B. Poonen on methods for finding rational points on curves of higher genus and one by F. Rodriguez-Villegas on Mahler measures and their interpretation as periods of motives. Some of the other main themes included:

- rational points on curves and higher dimensional varieties
- classical algebraic number theory (class groups, discriminants, Galois groups, ...)
- class number formulas, Stark's conjecture, algebraic K-theory
- analytic algebraic number theory
- points on curves over finite fields

As always in Oberwolfach, the atmosphere was ideal for exchanging ideas and conducting lively discussions.

Abstracts

Karim Belabas:

Computing $K_2\mathcal{O}_F$ for imaginary quadratic fields
(joint work together with Herbert Gangl)

Tate has given a strategy for computing $K_2\mathcal{O}_F$ for rings of integers in a number field. He and subsequent authors (Skałba, Qin, Browkin) have refined the method and were able to completely determine the structure of $K_2\mathcal{O}_F$ for a handful of imaginary quadratic fields. Using Tate's construction and ideas coming from the Hafner-Mc Curley algorithm to compute $(K_0\mathcal{O}_F)_{\text{tor}}$ together with $K_1\mathcal{O}_F$ (canonically isomorphic to $\text{Cl}(\mathcal{O}_F)$ and $\mathcal{O}_F^*$ respectively), we are able to compute $K_2\mathcal{O}_F$ in a systematic way. The algorithm produces

explicit generators for the tame kernel and an exponent for each of them. In all cases computed so far, the results agree with the predictions made assuming Lichtenbaum's conjecture, hence we expect the generators to be independent and the exponent to be the true order. For example:
Theorem: Let $F = \mathbb{Q}(\sqrt{-163})$, then $K_2\mathcal{O}_F = \{1\}$
Theorem: Let $F = \mathbb{Q}(\sqrt{-303})$, then $K_2\mathcal{O}_F = \langle\{2^{10}, \frac{37}{2} + \frac{3}{2}\sqrt{-303}\}\rangle$ and this symbol is 11-torsion. [We conjecture it is non trivial.]

Pilar Bayer:
Some computations on a family of curves of genus three

In the context or Arithmetic Algebraic Geometry, some invariants, like Green functions, Faltings δ, heights, etc. are attached to curves defined over number fields. They are rather intrincated and have been calculated in very few cases. We provided the J. Guàrdia approach to the explicit determination of these invariants for the curves

$$C_n : y^4 = x^4 - 2(2n-1)x^2z^2 + z^4,$$

where $n \in \mathbb{N}$ ($n \not\equiv 0, 1 \mod 2^5$).

The projective non-singular curves C_n are of genus three and their Jacobians, $J(C_n)$, split completely. Some of the arithmetical invariants of the curves C_n and those of the elliptic quotients of $J(C_n)$ are related in a simple way, so that a stable model of C_n and the modular height of $J(C_n)$ can be calculated. Others, as Green functions are more involved.

The dualizing sheaf (in the sense of Arakelov theory) was presented, as well as a numerical lower bound for the self-intersection in the case $n = 3$.

The curves C_n are a particular case of a family of curves that had been cosidered previously by Cassels.

Daniel J. Bernstein:
Counting rational points by brute force

There are exactly 42 rational points of height up to 21000000 with positive coordinates on the Fermat quartic surface. I explained in detail how to carry out such a computation. The same techniques apply in generality; my programs have been used to numerically check the Brauer-Manin-type conjectures for some cubic surfaces.

Frits Beukers:

Cyclotomic points on curves

Let Ω be the set of roots of unity. Let $f \in \mathbf{Z}[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$ be a Laurent-polynomial, irreducible over $\mathbf{Q}$. Consider the diophantine equation

$$f(x_1, \ldots, x_n) = 0 \quad \text{in } x_1, x_2, \ldots, x_n \in \Omega$$

Let N_f be the Newton polytope corresponding to f and suppose it has positive n-dimensional volume. We show that the number of solutions to our equations in the case $n = 2$ is bounded by $22Vol(N_f)$. At the same time there is an efficient algorithm to find these points. We discuss an application to Lie-symmetries of a class of partial evolution equations.

Nils Bruin:

Chabauty using elliptic curves applied to generalised Fermat equations

When considering pairwise prime solutions $x, y, z \in \mathbb{Z}$ of the equation

$$x^r + y^s = z^t$$

for fixed $r, s, t \in \mathbb{Z}_{>1}$ with $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} < 1$, one is led to consider the rational points of curves of genus > 1, as is proved in a paper by Darmon and Granville. In some cases (if $r = s$ and for some r and s that have a factor in common), it is possible to determine these curves explicitly. To determine the rational points on the curve, the following method is proposed.

Suppose we have a cover of curves $\Phi : \mathcal{D} \to \mathbb{P}_1$ over $\mathbb{Q}$ that factors through an elliptic curve E over a number field K. Thus, we have $\mathcal{D} \xrightarrow{\pi} E \xrightarrow{\phi} \mathbb{P}_1$ with $\phi \circ \pi = \Phi$. Consequently, we have that $\Phi(\mathcal{D}(\mathbb{Q})) \subset \phi(E(K)) \cap \mathbb{P}_1(\mathbb{Q})$. Now suppose that the rank r of $E(K)$ is smaller than the degree m of K and that we have a prime p that splits completely in K and that all involved objects have sufficiently nice reduction properties at p. The m embeddings $K \hookrightarrow \mathbb{Q}_p$ agree on $\mathbb{Q} \subset K$ and induce maps $\phi_i : E(K) \to \mathbb{P}_1(\mathbb{Q}_p)$ for $i = 1, \ldots, m$. If $G = G_0 + n_1 G_1 + \cdots + n_r G_r \in E(K)$ has $\phi(G) \in \mathbb{P}_1(\mathbb{Q})$, then we have that

$$\phi_i(G_0 + n_1 G_1 + \cdots + n_r G_r) = \phi_j(G_0 + n_1 G_1 + \cdots + n_r G_r)$$

for all i, j. If the G_k are sufficiently close (p-adically) to the identity element of E, then these equations can be expressed as power series in $n_1, \ldots, n_r$ with coefficients in $\mathbb{Z}_p$. Integral solutions to such power series equations can usually be bounded in number if $r < m$. Since E is compact in p-adic topologies, we can cover $E(K)$ with finitely many neighbourhoods of this form and thus get an upper bound on $\#(\phi(E(K)) \cap \mathbb{P}_1(\mathbb{Q}))$. Often, we can even get a sharp bound and thus determine the set exactly. We then just have to check for finitely many points whether they lift to rational points through Φ^{-1}.

If we have a curve $\mathcal{C}$ that does not cover an elliptic curve, then we can still try to determine the rational points by covering $\mathcal{C}(\mathbb{Q})$ by the rational points of finitely many unramified covers $\mathcal{D}$ of $\mathcal{C}$, that might cover elliptic curves. A nice example of this exists for curves of genus 2. If we embed such a curve in its jacobian and pull it back along the multiplication-by-2 homomorphism, we get a genus 17, degree 16 unramified cover $\mathcal{D}$ of $\mathcal{C}$. Apart from $\mathcal{C}$, such a curve covers 15 elliptic curves, correspondig to the 2-torsion points of the jacobian of $\mathcal{C}$.

Algebraically, if $\mathcal{C}$ is $Y^2 = F(X)$, where F is a square-free degree 6 polynomial, this method boils down to choosing a factorisation of F in a quadratic part Q and a quartic part R over a field extension K. Then there is a finite set of values δ in K such that for each $(x, y) \in \mathcal{C}(\mathbb{Q})$, there is such a δ and $y_1, y_2 \in K$ such that

$$\begin{aligned} \delta y_1^2 &= R(x), \\ \delta y_2^2 &= Q(x), \\ \pm y &= \delta y_1 y_2 \end{aligned}$$

holds. The elliptic curve E corresponds to the genus 1 curve $Y_1^2 = \delta R(X)$ and ϕ corresponds to X.

This method yielded the following results

Theorem: If $x, y, z \in \mathbb{Z}$ satisfy $x^2 \pm y^4 = \pm z^6$ and $\gcd(x, y, z) = 1$ then $xyz = 0$.

Theorem: The only integer, pairwise prime, solutions to $x^2 + y^8 = z^3$ are

$$(x, y, z) \in \{(\pm 1, 0, 1), (0, \pm 1, 1), (\pm 1549034, \pm 33, 15613)\}$$

Theorem: The only integer, pairwise prime, solutions to $x^8 + y^3 = z^2$ are

$$(x, y, z) \in \{(\pm 1, 0, \pm 1), (0, 1, \pm 1), (\pm 1, 2, \pm 3), (\pm 43, 96222, \pm 30042907)\}.$$

Theorem: If $x, y, z \in \mathbb{Z}$ satisfy $x^2 + y^4 = z^5$ and $\gcd(x, y, z) = 1$ then $xyz = 0$.

Theorem: The only integer, pairwise prime solutions to $x^2 - y^4 = z^5$ are

$$(x, y, z) \in \{(\pm 1, 0, 1), (0, \pm 1, -1), (\pm 122, \pm 11, 3), (\pm 7, \pm 3, -2)\}.$$

These methods and results are described in detail in the PhD-thesis "Chabauty methods and covering techniques applied to generalised Fermat equations" by the author.

Dongho Byeon:

Class number 1 criteria for totally real algebraic number fields

Let K be a totally real algebraic number field. Using Siegel's formula for the special values of Dedekind zeta function, we will give class number 1 criteria for K.

Herni Cohen:
Density of discriminants of number fields

Let G be a finite transitive subgroup of S_n, K be a number field, and

$$N_{K,n}(G,x) = \#\{L/K, \text{ of degree } n \mid \mathrm{Gal}(L^{\mathrm{gal}}/K) \cong G, N(\delta(L/K)) \le x\}$$

(up to ismorphisms) We want to estimate $N_{K,n}(G,x)$ as $x \to \infty$. This is known for $G = C_2$, C_3, and, up to a multiplicative constant, for any Abelian group G. For example,

$$N_{K,2}(C_2,x) \approx \frac{1}{2^{r_2}} \frac{\mathrm{Res}_{s=1}\,\zeta_K(s)}{\zeta_K(2)} x$$

This is in fact rather hard.

We give methods using Kummer theory that allow us to attack the problem for solvable G. Explicit computations have been made for $G = C_l$, $G = D_4$, $G = C_2 \times C_2$ and are in progress for $G = A_4$ and S_4.

Wright and Yukie obtain similar results using adelic integrals, which are not easy to compute explicitly.

In particular, it is now known that

$$N_{K,4}(D_4,x) \approx c_K x \quad \text{explicit } c_K$$

and

$$N_{K,4}(S_4,x) \approx d_K x \quad \text{explicit } d_K$$

(the preceding best result for S_4 was $O(x^{3/2})$). It is conjectured that

$$N_{\mathbb{Q},n}(x) \approx cx$$

for all n, perhaps with $c = \frac{1}{\zeta(n)}$ if one counts fields and étale algebras with appropriate multiplicities.

Claus Fieker:
On Knots and Norm Equations

Starting with an explicit example of a number field of relatve degree 20 over the 5^{ths} cyclotomic field, I briefly recalled methods to solve norm equations (the geometric method and the S-unit method) and sketched a procedure to compute norm groups of abelian extensions.

Using two independent methods due to Scholz and Tate, I showed how to compute the number knot

$$\delta_{K/k} := \{\text{local norms everywhere}\}/\{\text{global norms}\}$$

measuring the amount of failure of the Hasse-Norm-Theorem. Scholz gave a despription of $\delta_{K/k}$ as the Galois group of a certain central ray class field over a ray genus field. Furthermore he provides explicit construtions for the ideal groups involved.

Tate on the other hand gave the exact sequence

$$1 \to \delta_{K/k} \to H^2(G, \mathbb{Q}/\mathbb{Z}) \to \oplus H^2(G_p, \mathbb{Q}/\mathbb{Z})$$

By using the explicit isomorphism $H^2(\prod_i C_{n_i}, \mathbb{Q}/\mathbb{Z}) \cong \prod_{i<j} C_{(n_i,n_j)}$ and using the ideal groups to compute the decomposition groups G_p, I computed $\delta_{K/k}$ to be of order 2 in this case. Using S-units, I provided a generator.

By using a splitting argument, it was possible to produce a solution to the initial equation.

Eduardo Friedman:
Improving the unconditional discriminant bounds for number fields of small degree

Matias Atria has obtained improvements in the lower bound for the discriminant of a small degree number field by exploiting hypothetical violations of the Generalized Riemann Hypothesis. Indeed, if GRH holds, we have reasonably adequate lower bounds. So if we assume such a bound fails, we can assure the existence of a zero in the region D where a certain auxiliary function used by Odlyzko is negative.

Be varying this auxiliary function slightly, one can show that this zero ρ_0 lies in a small region at height approximately 2.2 above the real axis. One then exploits this zero by finding auxiliary functions that yield good bounds (unconditionally) given the existence of a zero in the region D.

The case $n = 8$, $r_1 = 6$ (n = degree, r_1 = number of real places) has been completely determined by Atria, checking all computer calculations rigorously. He obtained for this signature

$$|\text{disc}| > 9.05^8.$$

Compare this with the unconditional (previous) $|\text{disc}| > 8.97^8$ and the unconditional $|\text{disc}| > 9.27^8$.

Herbert Gangl:
Towards a higher class number formula

Dirichlet's class number formula for a number field F,

$$\zeta_F^*(0) = \frac{-h_F R_F}{w_F},$$

where h_F = class number, $w_F = \#\{\text{roots of } 1\}$ and R_F = Regulator of F, has been conjecturally generalized by Lichtenbaum in the famous *Lichtenbaum Conjecture* (LC): For $m > 1$:

$$\pi^{(m-1)d_m}\zeta_F^*(1-m) \stackrel{?}{=} 2^? \frac{\#K_{2m-2}\mathcal{O}_F}{\#(K_{2m-1}^{\text{ind}}\mathcal{O}_F)_{\text{tors}}} R_{m,F}$$

where $d_m = \begin{cases} r_1 + r_2, & m \text{ odd} \\ r_2, & m \text{ even} \end{cases}$, $K_n\mathcal{O}_F$ denotes Quillen's K-groups, and $R_{m,F}$ is the Borel regulator (the covolume of a certain lattice generated by $K_{2m-1}\mathcal{O}_F$ via the Borel regulator map) (The superscript "ind" denotes the indecomposable part.)

By making the pair ($K_{2m-1}\mathcal{O}_F$, Borel regulator map) explicit via Zagier's conjecture, namely replacing it by (m^{th} Bloch group, m-logarithm), we can numerically not only verify the plausibility of (LC), but also deduce conjectural orders (or at least divisibilities by larger primes, i.e. > 5) of $\#K_{2m-2}\mathcal{O}_F$, for which very little is known. Furthermore, the incompatibility with an alleged proof of a modified version of (LC) in the abelian case led to the discovery of a mistake in this proof, giving the experiments even a theoretical value.

Perhaps a mere coincidence is the following instance (suggested by the experiments):

$$1301 | \#K_4\mathbb{Z}[\zeta_{11}] \text{ and } 1301 | h^-_{11\cdot 12-1}$$
$$37 \cdot 61 | \#K_4\mathbb{Z}[\zeta_{13}] \text{ and } 37 \cdot 61 | h^-_{13\cdot 14-1}$$

where h_n^- denotes the relative class number for the n^{th} cyclotomic field over $\mathbb{Q}$.

Jürgen Klüners:

Recent Developments in Constructive Galois Theory.

(joint work together with Gunter Malle)

Until now, the inverse problem of Galois theory, i.e., the question whether every finite group occurs as the Galois group of a field extension of $\mathbb{Q}$, has not been solved. Even less is known in the direction of explicit results. Complete results for permutation groups of small degree were until now only known in degrees up to eleven. We encounter two types of problems. First, as mentioned above, not all the groups up to degree 15 were even theoretically known to occur as Galois groups over $\mathbb{Q}$. Secondly, there arises the practical problem how to come from theoretical existence results to explicit polynomials. An important tool in the constructions is a Galois group program which also yields the correct ordering of the roots, as provided by the computer algebra system Kant.

For nearly all transitive groups up to degree 15 we give methods to construct polynomials over $\mathbb{Q}$ and $\mathbb{Q}(t)$. We discuss the remaining cases and prove that there exist regular extensions of $\mathbb{Q}(t)$ for these groups. Altogether we prove that for all transitive groups G up to degree 15 there exists a polynomial $f \in \mathbb{Q}(t)[x]$ such that $\text{Gal}(f) = G$ and the extension is regular.

We have created a database with about 50000 polynomials over $\mathbb{Q}$ covering all transitive groups up to degree 15.

Kristin Lauter:
Improvements on the Weil-Serre-Oesterlé Upper Bounds for $N_q(g)$

Currently, the best known bounds on the number of rational points on an absolutely irreducible, smooth, projective algebraic curve of genus g defined over a finite field $\mathbb{F}_q$ generally come either from Serre's refinement of the Weil bound if the genus is small compared to q, or from the optimization of the explicit formulae if the genus is large.

This talk presented three methods for improving these bounds in both cases. The arguments used are the indecomposability of the theta divisor of a curve, Galois descent, and Honda-Tate theory. Examples of improvements on the bounds include lowering them for a wide range of small genus when $q = 8, 32, 2^{13}, 27, 243, 125$, and when $q = 2^{2s}$, $s > 1$. For large genera, isolated improvements are obtained for $q = 3, 8, 9$.

Franz Lemmermeyer:
Capitulation of Tate-Shafarevich groups

Let k denote a number field, let $\mathrm{E} : y^2 = x(x^2+ax+b)$ be an elliptic curve defined over k, and assume that the coefficients a, b are elements of a unique factorization domain R whose quotient field is k. Let $\phi : \mathrm{E} \longrightarrow \widehat{\mathrm{E}}$ denote the 2-isogeny associated to the subgroup of $\mathrm{E}(k)$ of order 2 generated by $(0,0)$, and let $\psi : \widehat{\mathrm{E}} \longrightarrow \mathrm{E}$ be its dual.

Realizing elements of $Ш(\mathrm{E}/k)[\phi]$ as torsors $\mathcal{T}(b_1) : N^2 = b_1M^4 - 2aM^2e^2 + b_2e^4$ that are everywhere locally solvable but do not have a nontrivial rational point (where $b_1, b_2 \in R$ are such that $b_1b_2 = a^2 - 4b$) we say that the class of $\mathcal{T}(b_1)$ in $Ш(\mathrm{E}/k)[\phi]$ capitulates in an extension K/k if $\mathcal{T}(b_1)$ has a K-rational point. Heegner's Lemma states that there is no capitulation of $Ш(\mathrm{E}/k)[\phi]$ in extensions K/k of odd degree. For quadratic extensions $K = k(\sqrt{d}\,)$ with $d \in k$ we show that the capitulation of $Ш(\mathrm{E}/k)[\phi]$ or $Ш(\widehat{\mathrm{E}}/k)[\psi]$ is related to the Mordell-Weil rank of the quadratic twist $\mathrm{E}^d(k) : dy^2 = x(x^2 + ax + b)$.

Franck Leprévost:
A tower of abelian surfaces related to the Kowalewski top
(joint work together with D. Markushevich)

Several curves of genus 2 are known, such that the equations of motion of the Kowalewski top are linearized on their Jacobians. One can expect from transcendental approaches via solutions of equations of motion in theta-functions, that their Jacobians are isogeneous. The paper focuses on two such curves: Kowalewski's and that of Bobenko–Reyman–Semenov-Tian-Shansky, the latter arising from the solution of the problem by the method of spectral curves. An isogeny is established between the Jacobians of these curves by purely algebraic means, using Richelot's transformation of a genus 2 curve. It is shown that this isogeny respects the Hamiltonian flows. The two curves are completed into an

infinite tower of genus 2 curves with isogeneous Jacobians.

Christian Maire:
Bound discriminants for number fields
(joint work together with Farshid Hajir)

For a number field k of degree n over Q, we define its root discriminant r_k as followed:

$$r_k = d_k^{1/n},$$

where d_k is the absolute value of the discriminant of k.

Now let α_n be the minimum of r_k for all totally imaginary fields of degree n over Q. Then, we put:

$$\alpha = \liminf_n \alpha_n.$$

In 1978, Martinet proved that $\alpha < 92.4$. Using Hilbert Tamely ramified Class field tower, we improve Martinet's estimate by showing that $\alpha < 82.2$.

Bjorn Poonen:
The method of Chabauty and Coleman

Chabauty proved around 1940(!) that if X is a curve of genus g over a number field k such that $\operatorname{rank}(\operatorname{Jac} X)(k) < g$, then $X(k)$ is finite. Coleman in 1985 showed that Chabauty's argument yields an explicit upper bound for $\#X(k)$. This method of Chabauty and Coleman, in conjunction with the Chevalley-Weil method of unramified covers, seems to be the best hope today for determining rational points on explicitly given curves of genus ≥ 2. In these two lectures, we give a survey of the method, explaining some recent improvements, and some of the difficulties in making it effective.

Fernando Rodriguez-Villegas:
Mahler Measures and L-functions

The Mahler Measure $M(p) = e^{m(p)}$ of a non zero Laurent polynomial $p \in \mathbb{C}[x_1, x_1^{-1}, \ldots, x_N, x_N^{-1}]$ is

$$m(p) = \frac{1}{(2\pi i)^N} \int_T \log|p(x_1, \ldots, x_N)| \frac{dx_1}{x_1} \ldots \frac{dx_N}{x_N}$$

where $T = \{(x_1, \ldots, x_N) \in \mathbb{C}^N \mid |x_1| = \cdots = |x_N| = 1\}$. In the 80's Smyth proved that

$$m(x + y + 1) = L'(\chi, -1)$$

where χ is the quadratic character of conductor 3. Recently Deninger showed how to view $m(p)$ as a Deligne period of a mixed motive for p non vanishing on T and Boyd made a number of numerical experiments like the following. For $k > 4$, $k \in \mathbb{Z}$

$$(*) \qquad m(x + \frac{1}{x} + y + \frac{1}{y} - k) \overset{?}{\approx}_{\mathbb{Q}^*} L'(E_k, 0)$$

($\approx_{\mathbb{Q}^*}$:= Sides differ by a non zero rational factor) where E_k is the elliptic curve determined by

$$x + \frac{1}{x} + y + \frac{1}{y} - k = 0$$

The purpose of this talk was to explain how Boyd's construction of polynomials of this type provides an element in $K_2(\mathcal{E}_k)$, where $\mathcal{E}_k$ is a Nèron model of E_k, and how $(*)$ is in fact a special case of the conjectures of Bloch and Beilinson.

Bart de Smit:
Permutation modules and Class Number Relations
(joint work together with Wieb Bosma)

$$\begin{array}{c} M \\ | \\ G \\ | \\ \mathbb{Q} \end{array}$$

X, X' finite G-sets. $K = \mathrm{Map}(X, M)$, $K' = \mathrm{Map}(X', M)$. If $\forall g \in G : \#X^g = \#X'^g$ then K and K' are products of numberfields with equal ζ functions: $\zeta_K = \zeta_{K'}$. We give an algorihm to compute bounds on the class number quotient h/h', and to produce formulas relating h/h' to a certain unit index.

Applications:

$$\frac{h(\mathbb{Q}(\sqrt[8]{a}))}{h(\mathbb{Q}(\sqrt[8]{16a}))} \in \{\frac{1}{2}, 1, 2\}$$

$$\begin{array}{ccc} & M & \\ A_4 & \triangleright & K_d \\ & \mathbb{Q} & d \end{array}$$

$$\frac{h(K_6)}{h(K_3)h(K_4)} \in \{\frac{1}{4}, \frac{1}{2}, 1\}$$

In both examples all possibilities occur.

Chris Smyth:
Remak's height
(joint work together with Arturas Dubickas)

We study the height

$$R(\alpha_1) = |a_0||\alpha_1||\alpha_2|^{\frac{d-2}{d-1}}|\alpha_3|^{\frac{d-3}{d-1}} \dots |\alpha_{d-1}|^{\frac{1}{d-1}}$$

"Remak's height", for an algebriac number α_1 with minimal polynomial $a_0 z^d + \cdots + a_d = \prod_{i=1}^{d}(z - \alpha_i)$. This height essentially appears in an inequality of Remak(1952). We find

sharp upper and lower bounds for $R(\alpha_1)$ in terms of the Mahler measure $M(\alpha_1)$. Analysis of the cases when these inequalities are equalities leads to the study of algebraic numbers lying with their conjugates on two circles. A full description of such numbers is given.

We also discussed a variant of the Mahler measure, the "Metric Mahler measure" $\mathrm{mmm}(\alpha)$ of an algebraic number α, defined by

$$\mathrm{mmm}(\alpha) = \inf_{\alpha=\beta_1\beta_2\ldots\beta_k} \sum_{i=1}^{d} m(\beta_i).$$

Here $m = \log M$. This gives rise to a metric $\mathcal{D}$ on $\bar{\mathbb{Q}}^*/\Omega$, Ω being the group of all roots of unity, defined by $\mathcal{D}(\alpha, \alpha') = \mathrm{mmm}(\alpha/\alpha')$. This metric gives the discrete topology on $\bar{\mathbb{Q}}^*/\Omega$ iff the answer to Lehmer's question is "yes", i.e. iff there is a $c > 0$ such that $m(\alpha) > 0 \implies m(\alpha) \geq c$.

David Solomon:
A p-adic Stark Conjecture at $s = 1$: Theory and Computations

Let

$$Z(s, d) := \sum_{n=1}^{\infty} \frac{\xi^n}{n^s}$$

where $\xi = e^{2\pi id/f}$, $f, d \in \mathbb{Z}$ $(d, f) = 1$ and $f > 1$. Then

$$Z(1, d) = -\log(1 - \xi) \text{ and } Z(1, d) + Z(1, -d) = -\log|(1 - \xi)(1 - \xi^{-1})|$$

Notice that $(1-\xi)(1-\xi^{-1})$ is a cyclotomic unit (or f-unit) in $\mathbb{Q}(\xi)^+ = \mathbb{Q}(f\mathbb{Z})$, the ray-class field to $\mathbb{Q}$ modulo the cycle $f\mathbb{Z}$.

Let K/k be an abelian extension of number fields and χ a character in $\mathrm{Gal}(K/k)^*$. The Stark Conjectures for the complex L-functions $L_{K/k}(s, \chi)$ at $s = 0$ can be seen as conjectural generalisations of this fact (via the functional equation). To see this, one first rewrites $L_{K/k}(s, \chi)$ in terms of certain generalisations of $Z(s, d)$ over k, which we call 'twisted zeta functions'. In the talk, we concentrated on the case where k is totally real and $K = k(\mathfrak{f})$ or $k(\mathfrak{f}+)$ for some ideal $\mathfrak{f} \lhd \mathcal{O}_{\|}$, $\mathfrak{f} \neq \mathcal{O}_{\|}$. Rather than stating the full complex conjecture, we wrote down a strictly analogous conjecture at $s = 1 \in \mathbb{Z}_p$ for the *p-adic* twisted zeta functions that can be obtained by p-adic interpolation of the complex versions on the set $\{1 - m : m \in Z_{>0}, (p-1)|m\}$ $(p \neq 2)$. Roughly speaking, their values at $s = 1$, suitably combined, should be given by a p-adic regulator of $\mathfrak{f}$-units in $k(\mathfrak{f})$, with values in $\mathbb{C}_p[\mathrm{Gal}(k(\mathfrak{f})/k)]$.

Further, for k real quadratic, we gave an explicit formula for computing these values to any p-adic precision by a geometrically-converging series. Finaly, an example was presented with $p = 3$, $k = \mathbb{Q}(\sqrt{37})$ and $\mathfrak{f} = 2(\mathcal{O})_{\|}$, so that $\mathrm{Gal}(k(\mathfrak{f})/\mathbb{Q}) = S_3$. We determined $\mathfrak{f}$-units u_1, u_2 in $k(\mathfrak{f})$ which satisfy the conjecture to 34 3-adic places in each coefficient of the

group-ring element. Moreover, u_1 and u_2 turn out to be free generators over $\mathbb{Z}[\mathrm{Gal}(k(\mathfrak{f})/k)]$ of the appropriate group of $\mathfrak{f}$-units. (This essentially determines their regulator). This and several more complicated examples, were calculated in joint work with Xavier-François Roblot.

HAROLD STARK:
The uniform abc-conjecture
(joint work together with Andrew Granville)

We investigate a variant of the abc conjecture wich is uniform over number fields. Notation: if $\alpha_1, \dots \alpha_n$ are in an algebraic number field K, not all zero, we set

$$H(\alpha_1, \dots, \alpha_n) = [\prod_v (\max_j \|\alpha_j\|_v)]^{1/[K:\mathbb{Q}]},$$

$$N(\alpha_1, \dots, \alpha_n) = [\prod_{\mathfrak{p} \in I} N(\mathfrak{p})]^{1/[K:\mathbb{Q}]},$$

where $I := \{\mathfrak{p} \mid \mathfrak{p}\text{does not divide all } \alpha_i\text{to the same power}\}$. We also set $\Delta_K = |\mathrm{disc}(K)|^{1/[K:\mathbb{Q}]}$.

uniform abc conjecture. There is a number $A > 0$ such that for any $\epsilon > 0$, if $a + b = c$ holds for non zero numbers in a field K, we have

$$(*) \qquad H(a,b,c) <<_\epsilon \Delta_K^{A+\epsilon} N(a,b,c)^{1+\epsilon}$$

and the implied constant depends only on ϵ and not on a, b, c or even K. Simple examples show that we require $A \geq 1$ in $(*)$. This leads to the *strong uniform abc conjecture.* We may take $A = 1$ in the uniform abc conjecture. Let $k = \mathbb{Q}(\sqrt{-d})$ where $-d$ is the discriminant of k and let $k(N)$ be the ray class field of $k \mod N$. We apply the uniform abc conjecture to the modular function $j(z)$ and the relation $(j(w) - 1728) + (1728) = (j(w))$ with $K = k(6)$ and $\Delta_K < 6d^{1/2}$. The result implies the class number of K grows fast enough that there are no Siegel zeros (for large d) and further, the result precisely matches what GRH says when $A = 1$. Thus we get an ininite family of fields of growing degree in which the strong uniform abc conjecture is precisely the right answer. In this application N comes out of the order of $H^{5/6}$ in $(*)$, since $j(w) - 1728$ is a square in $k(6)$ and $j(w)$ is a cube in in $k(6)$.

We also investigate the relation $(\lambda(w)) + (1 - \lambda(w)) = 1$ in $k(2)$ using the modular function $\lambda(w)$. Since $\lambda(w)$ and $1 - \lambda(w)$ are 2-units we have $N = O(1)$ in this case and so there is the possibility that this would furnish examples pushing A above 1. It turns out not to be the case. Using the explicit reciprocity law of complex multiplication, we find

$$H(\lambda(w), 1 - \lambda(w)) \approx H(j(w) - 1728, 1728, j(w))^{1/6}$$

and so the strong uniform abc conjecture is again at the exact boundary of our examples.

Michael Stoll:

Explicit p-decent for elliptic curves

Let p be an odd prime, and let E be an elliptic curve over a number field K. There is an explicit method for computing the p-Selmer group $\mathrm{Sel}^{(p)}(K,E)$, which is feasible if $p=3$ and $K=\mathbb{Q}$ and should become feasible if $p=5$ and $K=\mathbb{Q}$ with the availability of good relative class group and unit algorithms.

This method is based on the general despription given by Ed Schaefer of descent methods 'using functions on the curve' (Math. Ann. 1998) and on work by Djabri, Schaefer and Smart (Trans. AMS, to appear). The new part here (worked out jointly with Ed Schaefer) is to guarantee that what one computes is really the Selmer group and not just a supergroup of it.

Here is how it works. Let $\bar{A} = \mathrm{Map}(E[p]\setminus\{0\}, \bar{K})$; this is a $\bar{K}$-algebra with a Galois action (induced from the actions on $E[p]$ and on $\bar{K}$), and let $A = H^0(K,\bar{A})$. This is an étale algebra over K of degree p^2-1. Similarily, let $E[p]^\vee\setminus\{0\}$ be the set of affine lines in the $\mathbb{F}_p$-vector space $E[p]$ that do not contain the origin, and define $\bar{B} = \mathrm{Map}(E[p]^\vee\setminus\{0\}, \bar{K})$ and $B = H^0(K,\bar{B})$. There is an exact sequence of Galois modules,

$$0 \longrightarrow E[p] \xrightarrow{w} \mu_p(\bar{A})^{(1)} \xrightarrow{u} \mu_p(\bar{B})^{(1)} \longrightarrow E[p] \longrightarrow 0\,,$$

with $w : P \mapsto (Q \mapsto e_p(P,Q))$ and $u : \phi \mapsto (\ell \mapsto \prod_{P\in\ell}\phi(P))$. (Here the superscript (1) means that we are only considering maps ϕ from $E[p]\setminus\{0\}$ or $E[p]^\vee\setminus\{0\}$ to μ_p satisfying $\phi(a\cdot P) = \phi(P)^a$ for $a\in\mathbb{F}_p^\times$.) Let $\mathcal{K}$ be K or a completion K_v of K, and write $A_\mathcal{K} = A\otimes_K\mathcal{K}$, $B_\mathcal{K} = B\otimes_K\mathcal{K}$. Then from the exact sequence above we can deduce an explicit description

$$H^1(\mathcal{K},E[p]) \cong \ker(\tau)\cap\ker(u_*) \subset (A_\mathcal{K})^\times/((A_\mathcal{K})^\times)^p$$

where

$$\tau : (A_\mathcal{K})^\times/((A_\mathcal{K})^\times)^p \longrightarrow (A_\mathcal{K})^\times/((A_\mathcal{K})^\times)^p$$

and

$$u_* : (A_\mathcal{K})^\times/((A_\mathcal{K})^\times)^p \longrightarrow (B_\mathcal{K})^\times/((B_\mathcal{K})^\times)^p$$

are explicit homomorphisms, and the coboundary map

$$E(\mathcal{K}) \longrightarrow (A_\mathcal{K})^\times/((A_\mathcal{K})^\times)^p$$

is also explicit. This finally leads to a description of the Selmer group which is explicitly computable as long as we can do the usual kind of class group and unit computations in the various number fields that make up A and B.

Peter Swinnerton-Dyer:

Explicit calculation of the Brauer-Manin obstruction

Let V be for example a smooth rational surface defined over a number field k. It is conjectured (and in particular cases known) that the Brauer-Manin obstruction is the

only obstruction to the Hasse principle and to Weak Approximation on V. This makes it desirable to have an efficient method of computing the Brauer-Manin obstruction and (as a intermediate step) of computing $\mathrm{Br}(V)/\mathrm{Br}(k)$.

Take for example V to be a cubic surface, and let K be the least field of definition of the 27 lines on V - and hence also of $\mathrm{Pic}(\bar{V})$. There is an isomorphism

$$\mathrm{Br}(V)/\mathrm{Br}(k) \tilde{\to} H'(\mathrm{Gal}(K/k), \mathrm{Pic}(\bar{V}),$$

where the right hand side is computable with some effort; but one would have to consider a large number of cases because $\mathrm{Gal}(K/k)$ can be any subgroup of the group of order 71840 of permutations of the 27 lines which preserve incidence relations. Instead we proceed as follows. Let $n := [\mathrm{Gal}(K/k)]$ and let $\varphi : \mathrm{Gal}(K/k) \to \mathrm{Pic}(\bar{V})$ be a cocycle; then $n\varphi(g) = \alpha_0 - g\alpha_0$ where $\alpha_0 = \sum \varphi(g')$. Conversely if we choose α in $\mathrm{Pic}(\bar{V})$ and an integer $m > 0$ then $\varphi(G) = m^{-1}(\alpha - g\alpha)$ is an element of order exactly m in H' iff

1. $g\alpha \equiv \alpha \mod m\,\mathrm{Pic}(\bar{V})$ for all $g \in G$, and
2. there is no m' with $0 < m' < m$ and $m'\alpha \in \mathrm{Pic}(\bar{V}) + \mathbb{Q} \otimes \mathrm{Pic}(V)$.

The first condition can be more conveniently rewritten as follows. For $0 \leq r < m$ let S_r be the set of lines λ which satisfy $(\lambda \cdot \alpha) \equiv r \mod m$; then $\mathrm{Gal}(K/k)$ fixes each S_r.

For given m and α this condition tells one a great deal about $\mathrm{Gal}(K/k)$; and using symmetry one does not have to look at many values of α. For cubic surfaces, it turns out that the only possible values of m are 1, 2, 3, 4 and 9, and for $m > 1$ we get very straightforward neccessary and sufficient conditions on $\mathrm{Gal}(K/k)$. For example $[H']$ is even if and only if V contains a double-six defined over k whose individual sixes are not defined over k. Thus if $[\mathrm{Br}(V)/\mathrm{Br}(k)]$ is even the Hasse Principle must hold!

Provided that k contains the m^{th} roots of unity, one can now construct an Azumaya algebra of order m as a cyclic algebra (X, f), and $\mathrm{inv}_v(X, f)(P_v)$ is equal to the norm residue symbol $(f(P_v), X)_v$ for any v-adic point P_v on V.

Helena Verrill:

The L-series and Picard-Fuchs equation of some varieties

If $X \xrightarrow{\phi} \mathbb{P}^1$ is a fibred variety, defined over $\mathbb{Q}$, what is the relationship between the L-series of the middle cohomology of X and the period of the fibres?

A result of Stiensha says that for X given by $y^2 = f(x_1, \ldots, x_N)$ a double cover of $\mathbb{P}^N$, then if $P_N(T) = \det(1 - T\,\mathrm{Frob}_p\, H^N_{cris}(X) \otimes \mathbb{Q})$ for p a prime, and β_n a certain coefficient in $(f(x_1, \ldots, x_N))^{(n-1)/2}$, then $\beta_n + a_1\beta_{n/p} + a_2\beta_{n/p^2} + \cdots + a_k\beta n/p^k \equiv 0 \mod p^{\nu(n)}$ where $\nu(n)$ is the power of p in n, and $\beta_n = 0$ if $n \notin \mathbb{Z}$. In our examples, the β_n are the coefficients of a solution of the Picard-Fuhs differential equation of the fibration.

- Now take X to be a rigid Calabi-Yau 3-fold, so $H^3(X, \mathbb{Q}_e)$ is 2-dimensional

- take fibres $X_t := \phi^{-1}(t)$ to be smooth K3 surfaces, or products of elliptic curves, for almost all t
- take $\mathbb{P}^1 \equiv \Gamma \setminus \theta\ \Gamma$ some congruence subgroup, and t, the parameter of $\mathbb{P}^1$ given by $t(\tau)$ for t some modular function of weight 0 for M.

The Picard-Fuchs equation is a differential equation $\mathcal{F}$ satisfied by the periods, $\int_{\gamma_t} \omega_t$, $\omega_t \in H^0(X_t, \Omega_t)$, $\gamma_t \in H_2(X_t, \mathbb{Z})$. In the examples, $\mathcal{F}$ has a solution space $f(\tau)(\mathbb{C} \otimes \mathbb{C} \otimes \tau^2(\mathbb{C}))$, where $f(\tau)$ is a weight 2 modular form for Γ, and the Mellin transforn of the L-series is a weight 4 Hecke eigenform for Γ.

I have made calculations for 8 examples, and in each case found the relation

$$f\frac{q}{t}\frac{dt}{dq} = g(q) + Aq(q^B)$$

(for some A, B - in most cases these were zero). This relationship enables one to numerically compute the intermediate Jacobians of X. It turns out this relationship implies the congruence relation. We can prove more generally a kind of Atkin-Swinnerton-Dyer congruence result:

Theorem If

- t is a weight 0 modular function for a congruence subgroup Γ of level N,
- f is a weight k modular form for Γ, locally $f = \sum b_n t^n$
- g is a weight $k+2$ modular form for Γ, $g = \sum a_n q^n$, with $\sum \frac{a_n}{n^s} = \prod_{p \text{ good}} \frac{1}{1 - a_n p^{-s} + \epsilon_p p^{n+1-3s}} \prod_{p \text{ bad}} E_p$ and
- if $f\frac{q}{t}\frac{dt}{dq} = \sum_{d|M} m_d g(d\tau)$ (some $M \in \mathbb{Z}$)

then for $p \not| MN$, $b_n p^r - a_n b_n p^{r-1} + \epsilon_p p k - 1 b_n p^{r-2} \equiv 0 \mod p^r$ (if $m \notin \mathbb{Z}$, $b_n := 0$) $\forall r, n \in \mathbb{Z}$.

We can consider to what extend this result determines the L-series of X if the solution of the Picard-Fuchs equation is known.

Joseph L. Wetherell:

Curves with many points in every genus

(joint work together with A. Kresch and M. Zieve)

Let $\mathbb{F}_q$ be a finite field of characteristic $p > 0$. Define $N_q(g)$ to be the maximal number of $\mathbb{F}_q$ points on any curve over $\mathbb{F}_q$ of genus g. In this talk we discuss lower bounds on $N_q(g)$; that is, we exhibit curves in every genus with many points.

A simple construction in characteristics 2 and 3 shows that if $g_2 \geq (2p-1)g_1$ then $N_q(g_2) \geq N_q(g_1)$. From this we show that $\liminf \frac{N_q(g)}{g} > 0$. The proof of this latter result makes use of the families of good curves provided by Serre, Ihara, etc. It seems likely that

this result can be extended to other characteristics. In the mean time, we show that there are abelian covers of $\mathbb{P}^1$ with $O(\frac{g}{\log g})$ points in every genus.

Chaoping Xing:

Constructions of maximal function fields

Maximal function fields over finite fields show some interesting applications to coding theory and other subjects. Constructing maximal function fields has not only mathematical nature but also application importance. One way to construct maximal function fields is to look at the subfields of the Hermitian function field that is a well known function field. By studying the automorphism group of the Hermitian function field, we obtain a class of maximal function fields. In fact, all known maximal function fields so far are subfields of the Hermitian function field.

Reports and abstracts edited by: Claus Fieker, Berlin

Participants

Bayer, Pilar; Barcelona, email: bayer@cerber.mat.ub.es
Belabas, Karim; Orsay, email: Karim.Belabas@math.u-psud.fr
Bernstein, Daniel J.; Chicago, email: djb@cr.yp.to
Beukers, Frits; Utrecht, email: beukers@math.ruu.nl
Birch, Bryan J.; Oxford, email: birch@maths.oxford.ac.uk
Bosma, Wieb; Nijmegen, email: bosma@sci.kun.nl
Bruin, Nils; Leiden, email: bruin@wi.leidenuniv.nl
Byeon, Dongho; Seoul, email: dhbyeon@kias.re.kr
Cohen, Henri; Talence, email: cohen@math.u-bordeaux.fr
Couveignes, Jean-Marc; Talence, email: couveign@dmi.ens.fr, couveign@math.u-bordeaux.fr, couveig@univ-tlse2.fr
Cremona, John E.; Nottingham, email: cremona@maths.exeter.ac.uk
Diaz y Diaz, Francisco; Talence, email: diaz@math.u-bordeaux.fr
Fieker, Claus; Berlin, email: fieker@math.tu-berlin.de
Friedman, Eduardo; Santiago de Chile, email: friedman@abello.dic.uchile.cl
Gangl, Herbert; Bonn, email: herbert@mpim-bonn.mpg.de
Klüners, Jürgen; Heidelberg, email: klueners@iwr.uni-heidelberg.de
Lauter, Kristin; Bonn, email: lauter@mpim-bonn.mpg.de
Lemmermeyer, Franz; Saarbrücken, email: franz@athene.math.uni-sb.de
Lenstra, Jr., Hendrik W.; Berkeley, email: hwl@math.berkeley.edu
Leprévost, Franck; Berlin, email: leprevot@math.tu-berlin.de
Maire, Christian; Talence, email: maire@math.u-bordeaux.fr
Matiyasevich, Yuri; München, email: yumat@pdmi.ras.ru
Müller, Michael; Essen, email: mdm@exp-math.uni-essen.de
Olivier, Michel; Talence, email: olivier@math.u-bordeaux.fr
Pila, Jonathan; Kew East, email: pila@ms.unimelb.edu.au
Pohst, Michael E.; Berlin, email: pohst@math.tu-berlin.de
Poonen, Bjorn; Berkeley, email: poonen@math.berkeley.edu
Rodriguez-Villegas, Fernando; Austin, email: villegas@math.utexas.edu
Simon, Denis; Talence, email: desimon@math.u-bordeaux.fr
Skoruppa, Nils-Peter; Talence, email: skoruppa@math.u-bordeaux.fr
Smart, Nigel; Bristol, email: nsma@hplb.hpl.hp.com
de Smit, Bart; Leiden, email: desmit@wi.leidenuniv.nl
Smyth, Chris J.; Edinburgh, email: c.smyth@edinburgh.ac.uk
Solomon, David; London, email: solomon@mth.kcl.ac.uk
Stark, Harold M.; La Jolla, email: stark@math.ucsd.edu
Stevenhagen, Peter; Amsterdam, email: psh@wins.uva.nl
Stoll, Michael; Dösseldorf, email: stoll@math.uni-duesseldorf.de
Swinnerton-Dyer, Peter; Cambridge, email: hpfs100@newton.cam.ac.uk
Verrill, Helena; Bonn, email: verrill@mpim-bonn.mpg.de
Washington, Lawrence; College Park, email: lcw@math.umd.edu
Wetherell, Joseph L.; Los Angeles, email: jlwether@alum.mit.edu

Xing, Chaoping; Singapore, email: xingcp@comp.nus.edu.sg
Zagier, Don B.; Bonn, email: don@mpim-bonn.mpg.de
Zimmer, Horst Günter; Saarbrücken, email: zimmer@math.uni-sb.de

Tagungsteilnehmer

Prof.Dr. Pilar Bayer
Facultat de Matematiques
Universitat de Barcelona
Departament d'Algebra i Geometria
Gran Via 585

E-08007 Barcelona

Wieb Bosma
Mathematisch Instituut
Katholieke Universiteit Nijmegen
Toernooiveld 1

NL-6525 ED Nijmegen

Prof.Dr. Karim Belabas
Mathematiques
Universite de Paris Sud (Paris XI)
Centre d'Orsay, Batiment 425

F-91405 Orsay Cedex

Prof.Dr. Nils Bruin
Department of Mathematics and
Computer Science
Rijksuniversiteit Leiden
Postbus 9512

NL-2300 RA Leiden

Prof.Dr. Daniel J. Bernstein
Department of Mathematics
University of Illinois at Chicago
M/C 249, 322 SEO
851 S. Morgan Street

Chicago IL-60607-7045
USA

Dongho Byeon
School of Mathematics
Korea Inst. for Advanced Study
207-43 Cheongryangri-dong,
Dondaemun-gu

Seoul 130-012
KOREA

Prof.Dr. Frits Beukers
Mathematisch Instituut
Rijksuniversiteit te Utrecht
P. O. Box 80.010

NL-3508 TA Utrecht

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

F-33405 Talence Cedex

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

GB-Oxford OX1 3LB

Prof.Dr. Jean-Marc Couveignes
A2X
Universite de Bordeaux
351, cours de la Liberation

F-33405 Talence Cedex

Prof.Dr. John E. Cremona
Dept. of Mathematics
The University of Nottingham
University Park

GB-Nottingham , NG7 2RD

Jürgen Klüners
Interdisziplinäres Zentrum
für Wissenschaftliches Rechnen
Universität Heidelberg
Im Neuenheimer Feld 368

69120 Heidelberg

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

F-33405 Talence Cedex

Prof.Dr. Kristin Lauter
Microsoft Research
Bldg. #9/2289
1 Microsoft Way

Redmond , WA 98052
USA

Prof.Dr. Claus Fieker
Fachbereich Mathematik
Technische Universität Berlin
Straße des 17. Juni 136

10623 Berlin

Franz Lemmermeyer
Fachbereich 9 - Mathematik
Universität des Saarlandes
Postfach 151150

66041 Saarbrücken

Prof.Dr. Eduardo Friedman
Depto. Matematicas
Universidad de Chile
Casilla 653

Santiago de Chile
CHILE

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

Berkeley , CA 94720-3840
USA

Dr. Herbert Gangl
Max-Planck-Institut für Mathematik
Vivatsgasse 7

53111 Bonn

Prof.Dr. Franck Leprevost
Fachbereich Mathematik
Technische Universität Berlin
Straße des 17. Juni 136

10623 Berlin

Prof.Dr. Christian Maire
Mathematiques et Informatique
Universite de Bordeaux I
351, cours de la Liberation

F-33405 Talence Cedex

Prof.Dr. Michael E. Pohst
Fachbereich Mathematik - FB 3
MA 8 - 1
Technische Universität Berlin
Straße des 17.Juni 136

10623 Berlin

Prof.Dr. Yuri Matiyasevich
Lehrstuhl Effiziente Algorithmen
Institut für Informatik
TU München

80290 München

Prof.Dr. Bjorn Poonen
Department of Mathematics
University of California
at Berkeley

Berkeley , CA 94720-3840
USA

Michael Müller
Institut für Experimentelle
Mathematik
Universität-Gesamthochschule Essen
Ellernstr. 29

45326 Essen

Prof.Dr. Fernando Rodriguez-Villegas
Dept. of Mathematics
University of Texas at Austin
RLM 8.100

Austin , TX 78712-1082
USA

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

F-33405 Talence Cedex

Denis Simon
Mathematiques et Informatique
Universite de Bordeaux I
351, cours de la Liberation

F-33405 Talence Cedex

Jonathan Pila
6 Goldthorns Avenue

Kew East 3102
AUSTRALIA

Prof.Dr. Nils-Peter Skoruppa
Mathematiques et Informatique
Universite de Bordeaux I
351, cours de la Liberation

F-33405 Talence Cedex

Prof.Dr. Nigel Smart
Hewlett-Packard Laboratories
Filton Road, Stoke Gifford

GB-Bristol BS34 8QZ

Peter Stevenhagen
Fakulteit Wiskunde en Informatica
Universiteit van Amsterdam
Plantage Muidergracht 24

NL-1018 TV Amsterdam

Dr. Bart de Smit
Mathematisch Instituut
Rijksuniversiteit Leiden
Postbus 9512

NL-2300 RA Leiden

Michael Stoll
Mathematisches Institut
Heinrich-Heine-Universität
Gebäude 25.22
Universitätsstraße 1

40225 Düsseldorf

Dr. Chris J. Smyth
Dept. of Mathematics & Statistics
University of Edinburgh
James Clerk Maxwell Bldg.
King's Building, Mayfield Road

GB-Edinburgh , EH9 3JZ

Prof.Dr. Peter Swinnerton-Dyer
Isaac-Newton-Institute
Cambridge University
20 Clarkson Road

GB-Cambridge CB3 OEH

Dr. David Solomon
Department of Mathematics
King's College London
University of London
Strand

GB-London WC2R 2LS

Helena Verrill
Max-Planck-Institut für Mathematik
Vivatsgasse 7

53111 Bonn

Prof.Dr. Harold M. Stark
Dept. of Mathematics
University of California, San Diego
9500 Gilman Drive

La Jolla , CA 92093-0112
USA

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

College Park , MD 20742
USA

Prof.Dr. Joseph L. Wetherell
Dept. of Mathematics, DRB 155
University of Southern California
1042 W 36 Place

Los Angeles , CA 90089-1113
USA

Prof.Dr. Chaoping Xing
Department of Mathematics
National University of Singapore
Science Drive 2

Singapore 117543
SINGAPORE

Prof.Dr. Don B. Zagier
Max-Planck-Institut für Mathematik
Vivatsgasse 7

53111 Bonn

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

66041 Saarbrücken