Mathematisches Forschungsinstitut Oberwolfach

Report No. 33/2001

Explicit Methods in Number Theory

July 22nd – July 28th, 2001

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 computational methods used.

A 'mini-serie' of three 1-hour lectures was given by J.-F. Mestre about the AGM and about lifting Galois extensions. Two 1-hour lectures were given by D. B. Zagier about binary cubic the forms.

Some of the other main themes included:

- rational points on curves and higher dimensional varieties
- 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

Computing automorphisms of Galois number fields with supersolvable Galois groups

B. Allombert

We describe an algorithm for computing the Galois automorphisms of a Galois extension with supersolvable Galois group which improves on an algorithm of Klüners. This is much faster in practice than algorithms based on LLL or factorization. Our implementation of the algorithm in PARI has enabled us to compute automorphisms of a number field of degree 336.

Cubic forms, cubic rings and cubic fields

K. Belabas

We present four applications of the theory of integral binary quadratic forms: a short proof of Davenport and Heilbronn's theorem characterizing classes of forms associated to maximal orders, density results for cubic fields discriminants and 3-torsion of class groups of quadratic fields (Davenport-Heilbronn), a formula for the generating series associated to the cubic orders belonging to a given field (due to Datskovsky and Wright using more elaborate methods), and finally prove that the smallest known quadratic field with 3-rank equal to 5 (found by Quer) is indeed the smallest existing one.
(*An introduction to this talk was given by D. B. Zagier*)

Finding polynomial values of small height

D. J. Bernstein

There is a fast algorithm that, given a nonzero polynomial $f \in \mathbf{Q}[x]$ find all $r \in \mathbf{Q}$ such that both r and $f(r)$ have small height. Typical applications: finding small roots of a monic polynomial in $(\mathbf{Z}/n)[x]$ (Hastad 1985; Vallée, Girault, Toffin 1988; Coppersmith 1996; Howgrave-Graham 1997); finding high-power factors of n (Boneh, Durfee, Howgrave-Graham 1999); correcting errors far beyond half the minimum distance of a code (Sudan 1997; Goldreich, Ron, Sudan 1998; Guruswami, Sudan 1999; Boneh 2000); and finding smooth values of a monic polynomial (Boneh 2000).

Cyclic covers of hyperelliptic curves

N. Bruin

(joint work with Victor Flynn)

We examine the structure of the Jacobian of an unramified cyclic cover of a hyperelliptic curve. We use it to determine the rational points on a hyperelliptic curve through covering collections and Chabauty techniques.

In particular, for a degree 3 unramified cyclic cover D of a genus 2 curve C, we find that the cover $D/\mathbf{P}^1$ induced by the hyperelliptic cover C, factors through three generically conjugate, genus 1 subcovers F_1, F_2, F_3. As it turns out, these curves can be defined over the base field and are all isomorphic. Furthermore, the three maps from D to F are not all independent. We find that the rational points on D map to the L-rational points on

$E = \mathrm{Jac}(F)$ with trace 0 and rational image on $\mathbf{P}^1$. This allows application of elliptic curve Chabauty.

Indivisibility of class numbers of real quadratic fields

D. Byeon

Let $D > O$ be the fundamental discriminant of a real real quadratic field, and $h(D)$ its class number. In this talk, we show that for any prime $p > 3$, we have $\#\{0 < D < x \mid h(D)$ is not divisible by $p\} \gg_p \sqrt{x}/\log x$.

The Jacobi problem for graphs and related computational issues

J.-M. Couveignes

When one considers the Jacobi problem for a curve defined over a complete discrete valuation field, one is lead (through the theory of Neron models) to the study of intersection graphs of special fibers.

This motivates the introduction of an adapted cell decomposition of the cohomology of a graph which we call the Kirchov complex of the graph $\mathcal{G}$. There is also an integration map

$$\phi \colon S^g\mathcal{G} \to H^1(\mathcal{G}, \mathbf{R})$$

where g is the genus of the graph and $S^g\mathcal{G}$ the g-th symmetric product. This Jacobi map has a unique continuous section (in contrast with the classical Jacobi map for algebraic curves). This means that the Jacobi problem has a canonical solution.

A complete Solution of $X^2 + Y^3 + Z^5 = 0$

J. Edwards

This talk shows how to generate a finite list of homogeneous forms G_i, H_i, F_i in $\mathbf{Z}[s, t]$ satisfying:

$$G_i^2 + H_i^3 + F_i^5 = 0$$

with the following property. If $X, Y, Z \in \mathbf{Z}$ satisfies:

$$X^2 + Y^3 + Z^5 = 0 \quad \text{with} \quad \gcd(X, Y, Z) = 1$$

then there is an index i, and $s_0, t_0 \in \mathbf{Z}$ such that:

$$X = G_i(s_0, t_0), \quad Y = H_i(s_0, t_0), \quad Z = F_i(s_0, t_0).$$

Before this result no feasible algorithm to produce such a list was known to exist.

Curves of genus 2 and subgroups of rank at most 1

N. D. Elkies

We report on various constructions, computations, conjectures and questions concerning subgroups of rank 0 or 1 in the Jacobians J of curves C of genus 2. Some examples follow.

The moduli space for C with 3 Weierstrass points and a 5-torsion element of J is rational (with an explicit parametrization; thanks to rationality of elliptic modular curve $X_1(10)$!).

The moduli space for C with all Weierstrass points rational as well as points P, Q and a degree-1 divisor D such that $2D \sim P + Q$, is a hyperplanes complement in $\mathbf{P}^5$. The

Galois group $\mathrm{ASp}_4(\mathbf{Z}/2\mathbf{Z}) \cong W(D_6)/\{\pm 1\}$ acts linearly by signed permutation matrices. [A Shioda-Usui "excellent family."]

The curve $y^2 = x^6+4x^4+10x^3+4x^2-4x+1$ has minimal $\mathrm{Aut}(C)$ but four non-Weierstrass point pairs $\{P, \iota P\}$ such that $(P) - (\iota P)$ is torsion; namely those with $x = \infty, 0, \pm 1$. These generate a 39-element torsion subgroup of the simple abelian surface J. Calculus nightmare: $\int (39x^2 + 9x - 1)\, dx/y$ is

$$15 \log |y + x^3 + 2x + 5| + 3 \log |y + 5x^3 + 12x^2 + 10x + 1| + \log |y + x^3 + 2x - 1| + C.$$

Also: $y^2 = (3x + 4)(x^4 + 5x^3 + 8x^2 + (19/4)x + 1)$, with J simple and $((-2, 1)) - (\infty)$ of order 40; two simple J's with 34-torsion, and a family over $\mathbf{Q}(t)$ with 32-torsion; and a 31-torsion subgroup for $y^2 + (x^3 - 1)y = x^6 - x^5 + 5x^4 + 6x^2 + 5x + 1$ generated by points over $\mathbf{Q}(\cos 2\pi/7)$.

For odd $n_i > 0$ ($i = 1, \ldots, 4$) consider curves C with nontorsion $D \in J$ and points P_i such that $[(P_i) - (\iota P_i)] = n_i D$. Such C are often parametrized by rational curves. For instance, if $(n_1, n_2, n_3, n_4) = (3, 5, 17, 21)$ then C is $y^2 = (x^3 - x + t(x^2 - x + 1))^2 - 4t(x^2 - x)$ with $P_i = (\infty, \infty^3)$, $(0, t)$, $(1, -t)$, $(-t, -t^2)$. Some other choices of n_i yield interesting elliptic curves. For instance, $(1, 5, 13, 45)$ and $(1, 5, 13, 51)$ are parametrized by the curves of conductor 37 and 446 of rank 1 and 2.

Hence find many (C, D) such that $nD = [(P) - (\iota P)]$ has 5 solutions. Once we get a bonus sixth point:

$$y^2 + (5x - 3)y = x^2(x + 1)^2(x - 1)(x - 3),$$

with the point pairs at $x = \infty, 0, 1, -1, 3, 1/2$ corresponding to $n = 1, 5, 13, 29, 61, 83$. That's all by Chabauty mod 7 (where $83D \equiv 0$).

Conjecture: even over $\mathbf{C}$, there are only finitely many curves C and nontorsion D such that $nD = [(P) - (\iota P)]$ for more than 5 positive odd n. Are there ever 7 solutions? Is there even another case of 6?

Calculation of the homology of $\mathrm{GL}(n, \mathbf{Z})$

H. Gangl

(joint work with Philippe Elbaz-Vincent and Christophe Soulé)

Voronoï proved—via his reduction theory of N-ary quadratic forms—that there is a finite CW complex on "perfect forms" that computes the homology of $\mathrm{GL}_N(\mathbf{Z})$. Jaquet has given a complete list of perfect forms for $N \leq 7$, together with their "neighbouring cells". This allows in principle to compute the associated CW complex V_N (by also exploiting algorithms of Souvignier), and we obtain the following results (so far only for $N \leq 6$):

Theorem. The homology of V_N for $N = 5$ and $N = 6$ is given by

$$H_n(V_5(\mathbf{Z}), \Lambda_5) = \begin{cases} \Lambda_5 & \text{if } n = 9 \text{ or } 14, \\ 0 & \text{otherwise,} \end{cases}$$

$$H_n(V_6(\mathbf{Z}), \Lambda_6) = \begin{cases} \Lambda_6 & \text{if } n = 10, 11 \text{ or } 15, \\ 0 & \text{otherwise,} \end{cases}$$

where $\Lambda_5 = \mathbf{Z}[\frac{1}{2}, \frac{1}{3}, \frac{1}{5}]$ and $\Lambda_6 = \mathbf{Z}[\frac{1}{2}, \frac{1}{3}, \frac{1}{5}, \frac{1}{7}]$.

This implies results for the homology of $\mathrm{GL}_N(Z)$ with coefficients in the "Steinberg module" St_N (the latter is associated to the spherical Tits building of SL_N over $\mathbf{Q}$).

Explicit computation of the group generated by the Weierstrass points of some plane quartics

M. Girard

We compute the group generated by the Weierstrass points of some particular plane quartics. Since there exists a stratification of the moduli space of curves of genus three depending on the number of hyperflexes—that is, points where the tangent line meets the curve with multiplicity 4—it enables us to deduce some bounds on the rank and some estimation on the torsion part for a generic quartic in each stratum.

Computing the tame kernel

R. P. Groenewegen

The tame kernel is defined as the kernel of some explicit map from the K_2 of a number field to a direct sum of unit groups of residue class fields. It is a finite group and we are interested in finding explicit generators and relations for it. In this talk we give a bound that is used to find generators of the tame kernel and we explain that the tame kernel is computable.

Hilbert-Picard modular cusps and special values of L-functions

P. E. Gunnells

(joint work with Robert Sczech and Jacob Sturm)

Let $F/\mathbf{Q}$ be a totally real number field of degree n, let $M \subset F$ be a rank n lattice, and let $V \subset O_F^\times$ be a finite-index subgroup of the totally positive units stabilizing M. We consider the special values

$$L(M,V;s) := \sum_{\mu \in (M-\{0\})/V} N_{F/\mathbf{Q}}(\mu)^{-s}, \quad s = 1,2,3,\dots .$$

Satake conjectured a connection between these special values and intersection numbers of divisors on toroidal resolutions of Hilbert-Picard modular cusps.

We prove this conjecture by explicitly summing the L-series in terms of data attached to the rational polyhedral fans defining the resolutions. In particular one can see explicitly how the relevant intersection numbers contribute to the L-values.

Fundamental unit computation in practice

M. J. Jacobson

(joint work with Hugh Williams)

Let $K = \mathbf{Q}(\sqrt{\Delta})$ be a real quadratic field. The most efficient algorithm for computing the regulator R of K in practice has subexponential complexity and is based on the self-initializing quadratic-sieve factoring algorithm. Unfortunately, the correctness of regulators produced by this algorithm is conditional on the Generalized Riemann Hypothesis (GRH)—the best that can be guaranteed unconditionally is a multiple of the regulator. In contrast, the best algorithm for computing R unconditionally has complexity $O(\Delta^{1/5+\varepsilon})$ under the GRH. We present a new algorithm which, given a multiple S of the regulator, computes R deterministically and unconditionally in time $O(S^{1/3+\varepsilon})$. Our algorithm is parallelizable, and, unlike other algorithms for computing R, only uses integer arithmetic. Combined with the subexponential algorithm, this yields a Las Vegas algorithm which computes R in expected time $O(\Delta^{1/6+\varepsilon})$. Although the runtime of this algorithm is conditional on the GRH, the correctness of R is unconditional. Computational results are presented which clearly demonstrate the efficiency of our algorithm.

Counting Galois extensions of number fields

J. Klüners
(joint work with Gunter Malle)

Let k be a number field and G be a finite group. We define

$$Z(k,G;x) := \left|\{K/k : \mathrm{Gal}(K/k) = G, |N_{k/\mathbf{Q}}(d_{K/k})| \leq x\}\right|.$$

We report about a conjecture of Gunter Malle that describes explicitly the asymptotic behaviour of that function. The conjecture is known to be true for all Abelian groups and some small groups like S_3 and D_4. In this talk we show that the conjecture is true for all nilpotent groups. The proof can be reduced to Kummer extensions and the study of Brauer embedding problems.

Computational aspects of Shimura curves

D. Kohel

We report on the current state of algorithms and computations for the Shimura curves $X_0^D(m)$ associated to an Eichler order $\mathcal{O}$ in a quaternion algebra of discriminant D (and index m in a maximal order). In particular we focus on two approaches to the study of these curves: (1) through the supersingular divisor group of the reduction modulo $p|m$, and (2) through hyperbolic geometry and particularly the problem of computing a fundamental domain for the group $\Gamma_0^D(m)$ of norm 1 units under its action on the upper half plane $\mathcal{H}$. The latter approach is part of joint work with Helena Verrill, based on similar work and computational tools for congruence subgroups of $\mathrm{SL}_2(\mathbf{Z})$.

The supersingular divisor group can be effectively modelled in terms of left quaternion ideals over a definite Eichler order $\mathcal{R}$ in a quaternion algebra of discriminant Dp, following the *Méthode des graphes* of Mestre and Oesterlé (which uses the equivalent category of supersingular elliptic curves) and the work of Pizer on computing modular forms via quaternions. Applications include the computation of L-functions of simple isogeny factors of the Jacobian of $X_0^D(m)$ and computing component groups of factors of $J_0(N)$ (see Kohel and Stein, ANTS IV, 2000). Progress on an algorithm for computing fundamental domains for Shimura curves was also presented, with examples. The approach through explicit modular forms and functions on Shimura curves, and the computation of models of Shimura curves have yet to be treated by the author (refer to the article of Elkies in the ANTS III proceedings for results in the latter direction). The book of Vignéras on quaternion algebras is the definitive background reference on the subject.

Some analytic problems for elliptic curves

E. Kowalski

Let $E/\mathbf{Q}$ be an elliptic curve and p a prime of good reduction. The finite group of points on E modulo p is of the type $\mathbf{Z}/d_1\mathbf{Z} \times \mathbf{Z}/d_1d_2\mathbf{Z}$ for some well-defined invariants d_1 and d_2.

We consider the average sum

$$S(X) = \sum_{p \leq X} d_1(p) = \sum_{p \leq \sqrt{X}+1} \varphi(d)\pi_E(X; d, 1)$$

where $\pi_E(X; d, 1)$ is the number of primes $p \leq X$ which are totally split in the d-torsion extension $\mathbf{Q}(E[d])/\mathbf{Q}$. Let G_d be the Galois group of this extension.

In the study of the behavior of this sum as $X \to +\infty$ we are led to various problems:
(1) Is it true that, if E has no CM, then

$$S(X) \sim c_E \operatorname{li}(X) \text{ as } X \to +\infty \text{ where } c_E = \sum_{d \geq 1} \frac{\varphi(d)}{|G_d|}.$$

(2) In studying Problem 1, there arises the possibility that $d_1(p)$ be "abnormally large," i.e., that p be split in $\mathbf{Q}(E[d])$ when the main term $p/|G_d|$ of the Chebotarev Density Theorem is < 1.

What is the distribution of primes p satisfying this condition? Are there infinitely many or not?

(3) Primes $p < q$ with $d = d_1(p) = d_1(q)$ rather large must be separated by at least $d^2/2$ *if* p and q are not E-twins, in the sense that E has as many points modulo p and q, $|E_p(\mathbf{Z}/p\mathbf{Z})| = |E_q(\mathbf{Z}/q\mathbf{Z})|$. What is the distribution of primes p which have at least one E-twin? Heuristics and numerical computations indicate that the number $J(X)$ of those $\leq X$ should be of order of magnitude $X/(\log X)^2$, comparable to that expected from ordinary twin primes.

When E has CM, the definition still makes sense. In this case one can conjecture that

$$\sum_{p \leq X} m(p)^k \sim c'_{E,k} X (\log X)^{2^k - k - 2} \text{ as } X \to +\infty$$

and prove upper bounds of the correct order of magnitude by sieve methods in $\operatorname{End}(E) \otimes \mathbf{Q}$. Here $m(p)$ is the number of primes which are twins of E.

(4) If E has no CM, is it true that

$$m(p) \ll_\varepsilon p^\varepsilon$$

for any $\varepsilon > 0$?

Zeta functions over nearly finite fields

H. W. Lenstra, Jr.
(joint work with Daqing Wan)

A field K is called *nearly finite* if it is, for some prime number ℓ, the maximal ℓ-extension of a finite field k. Let Y be a scheme of finite type over such a field K. Then, as shown in the lecture, one can meaningfully define, for each $n \in \mathbf{Z}$, $n \geq 1$, $n \not\equiv 0 \bmod i$, an ℓ-adic integer $a_n(Y)$, that may be thought of as the number of closed points of Y that have degree n over K. The zeta function $\mathrm{Z}(Y)$ is then defined as the power series $\prod_{n \geq 1, \ell \nmid n} (1 - T^n)^{-a_n(Y)}$ in $1 + T\mathbf{Z}_\ell[[T]]$. It is a rational function, all of whose zeroes and poles are roots of unity of order coprime to ℓ. If X is a scheme of finite type over k (with k as above) with $Y \cong_K X_K$, then knowledge of $\mathrm{Z}(Y)$ is equivalent to knowing the coefficients of the traditional zeta function $\mathrm{Z}(X/k)$ modulo ℓ.

Counting points on elliptic curves with AGM

J.-F. Mestre

Let $\tilde{E}$ be an elliptic curve over $\mathbf{F}_{2^d}$. Using Satoh's idea to use the canonical lifting of $\tilde{E}$ (supposed ordinary), we give an algorithm, which imitates the usual AGM, to

(1) obtain the canonical lift of E.

(2) compute $\#\tilde{E}(\mathbf{F}_{2^d})$.

The algorithm is:

(a) Choose any lifting of $\tilde{E}$ over K, where $K/\mathbf{Q}_2$ is unramified of degree d.

(b) Write $\tilde{E}$ as $y^2 = x(x-a^2)(x-b^2)$ with $b/a \equiv 1(8)$.

(c) Consider the AGM sequence

$$[a_{n+1}, b_{n+1}] = [\frac{a_n + b + n}{2}, \sqrt{a_n b_n}],$$

where $\sqrt{a_n b_n} = a_n \sqrt{b_n/a_n}$. $(\sqrt{1+\cdots} = 1(4))$

(d) $E_n\colon\ y^2 = x(x-a_n^2)(x-b_n^2)$ is such that $j_{\mathrm{End}} \to j$, the j-invariant of the canonical lifting of $\tilde{E}$.

(e) Take the integer α, with $|\alpha| < 2{\cdot}2^{d/2}$, nearest to $\frac{a_d}{a_{2d}} + 2^d \frac{a_{2d}}{a_d}$. Then $\#\tilde{E}(\mathbf{F}_{2^d}) = 2^d + 1 - \alpha$.

Genus 2 curves and the AGM

J.-F. Mestre

We give an analogue of the preceding algorithm to obtain the number of points on a curve of genus 2 over $\mathbf{F}_{2^d}$. Let $\tilde{C}/\mathbf{F}_{2^d}$ be of genus 2, with ordinary reduction.

Take any lifting of $\tilde{C}$ over K (with definition in the preceding talk). Write $C_0\colon\ y^2 = f(x) = p_1(x)p_2(x)p_3(x)$, with p_1, p_2, p_3 squares modulo 2 (we have to consider an extension of K to do that), $p_1 \equiv (x-x_i)^2 \bmod 2$. If $[P,Q] = P'Q - PQ'$, consider $Q_1 = [p_2, p3]$, $Q_2 = [p_3, p_1]$, $Q_3 = [p_1, p_2]$ and put $C_1\colon\ \Delta y^2 = Q_1 Q_2 Q_3$, where Δ is the determinant of $(p_1 p_2 p_3)$ in the basis $1, x, x^2$.

The curves C_{nd} converge to the canonical lifting of $\tilde{C}$. Up to 2^d-precision, C_d and C_{2d} are isomorphic; let

$$(x,y) \longmapsto \left(\frac{ax+b}{cx+d}, \frac{\lambda y}{(cx+d)^3}\right)$$

be such an isomorphism. The characteristic polynomial of Frobenius is $x^2 P_m(x) P_m(2^d/x)$, where P_m is the characteristic polynomial of m (or more precisely of the integer approximation of it).

Lifting of Galois extensions from K to $K(T)$

J.-F. Mestre

Let K be a field of characteristic 0, G a finite group, and L/K an extension of K of Galois group G. A natural question is: does there exist a regular extension M of $K(T)$, where T is an indeterminate of Galois group G such that, for $T=0$, we recover the initial extension L/K?

In the case where $G = \mathrm{PSL}_2(\mathbf{F}_2)$, the answer is yes; more precisely, there exist H in $k[a_0, a_1, \ldots, a_6]$, nonzero, such that, if $P = a_0 + a_1 X + \cdots + a_6 X^6 + X^7$ is in $K[X]$ is such that $H(a_0,\dots,a_6)\neq 0$, and if $\mathrm{Gal}(P)$ is included in $\mathrm{PSL}_2(\mathbf{F}_2)$, there exist Q in $K[X]$ such that $\mathrm{Gal}_{K(T)}(P-TQ)=\mathrm{PSL}_2(\mathbf{F}_2)$.

This is based on the following assertion about correspondences: let P_i and D_j be the seven points and lines of the projective plane over $\mathbf{F}_2$, and $i\to j$ the corresponding incidence relations; let $x_1,\dots,x_7$ be indeterminates; there exist $y_1,\dots y_7$ in $\mathbf{Z}[x_1,\dots,x_7]$ and F in $\mathbf{Z}[X,Y]$ of bidegree 3-3 such that $F(x_i,y_j)=0$ if and only if $i\to j$ (we note this $(x_1,\dots,x_7)\to(y_1,\dots,y_7)$).

This gives also a result analogous to Poncelet theorem: for instance, if F in K[X,Y] of bidegree 3-3 is sufficiently general and is such that there exist *one* such configuration $(a_1,\dots,a_7)\to(b_1,\dots,b_7)$, then, for *any* x_1 in $\mathbf{P}^1$, we obtain a such configuration $(x_1,x_2,\dots,x_7)\to(y_1,\dots,y_7)$.

Explicit 3-descent over $X(3)$

C. H. O'Neil

Given an elliptic curve E over a field, we explicitly perform 3-descent assuming full 3-torsion on E. With such an assumption, elements of the Selmer group can be represented as pairs (a,b) in the base field mod cubes. Moreover, (a,b) being an element of the Selmer group implies that the corresponding Hilbert symbol is trivial, which lets us represent b as a norm from an extension of the base field by the cube root of a. We use this representation in the formula for a model for (a,b).

Polylogarithms over real quadratic number fields

R. Sczech

We consider partial Hecke L-functions in real quadratic number fields which are associated to a sign character of the type $v(a)=\mathrm{sign}(a)$ or $v(a)=\mathrm{sign}(a')$. These L-functions vanish at $s=0,-1,-2,-3,\dots$, so their first order derivative at those points are of natural interest. We present numerical examples for the conjecture that these derivatives are (suitably normalized) polylogarithms evaluated on higher analogs of Stark units belonging to Bloch groups of abelian extensions of the underlying real quadratic number field.

The index of nonmonic polynomials

D. Simon

We show that the index of nonmonic polynomials gives the same information on the ring of integers in a number field as monic polynomials. In particular, we generalize a result of M.-N. Gras by proving that almost all cyclic extensions of $\mathbf{Q}$ of prime degree cannot be generated by a (nonmonic) polynomial with index 1. More precisely, we prove that this index goes to infinity with the conductor.

Explicit formulas for the Mahler measure of a family of 3-variable polynomials

C. J. Smyth

I give an explicit formula for the Mahler measure $m(P_{abc})$ of the family of 3-variable Laurent polynomials

$$P_{abc}(x,y,z)=a+bx^{-1}+cy+(a+bx+cy)z$$

where a, b, c are real. These formulas involve dilogarithms and trilogarithms. For instance, one special case is, for $c \in [0,1]$

$$m(P_{01c}) = \frac{2}{\pi^2}(\mathrm{Li}_3(c) - \mathrm{Li}_3(-c)).$$

Many digits of derivations of p-adic L-functions at $s = 0$

H. M. Stark

In the proceedings of the 1985 Montreal number theory conference, I showed how to create a p-adic Dirichlet series which interpolates the values of the Hurwitz zeta function at negative integers. This allows the calculation of the derivative of the p-adic Dirichlet series at $s = 0$ in terms of the p-adic logarithm of the p-adic Γ-function and simultaneously provides the formulas for accurately computing the result to many p-adic digits. In this talk we investigate the same process for the double series

$$\mathrm{Z}(s, w \mid \omega_1, \omega_2) = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} (m\omega_1 + n\omega_2 + w)^{-s}.$$

The resulting p-adic interpolation leads to a derivative at $s = 0$ of a p-adic double Γ-function and formulas for accurately calculating its values. This is the first step aimed at p-adic L-functions for quadratic fields.

Some modular degree and congruence modulus computations

W. A. Stein

Let E be an elliptic curve over $\mathbf{Q}$ that is an optimal quotient of $J_0(N)$, where N is the conductor of E. Two closely related invariants attached to E are the congruence modulus and modular degree. In this talk, I will report on some of my computations of these invariants that answer an open question, and I will present some recent results and observations of Ken Ribet.

Computing primitive root densities

P. Stevenhagen

(joint work with Pieter Moree and Hendrik Lenstra)

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 admit a simple 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.

Extreme Chabauty

M. Stoll

We present a result giving a bound on the number of rational points mapping into a given small-rank subgroup of the Mordell-Weil group of a twist of a given curve over a number field. Among others, this implies the following.

Theorem. Let $C\colon\ y^2 = f(x)$ be a hyperelliptic curve of genus $g \geq 2$ over $\mathbf{Q}$. Then for all but finitely many $d \in \mathbf{Q}^\times/(\mathbf{Q}^\times)^2$, the following is true. Any set of $n \leq g$ rational points on the quadratic twist C_d that is disjoint from its image under the hyperelliptic involution generates a subgroup of rank n in the Jacobian of C_d.

Theorem. Let $f(x, y) \in \mathbf{Z}[x, y]$ be homogeneous of degree $n \geq 3$ and squarefree. Then for all but finitely many nth power free $h \in \mathbf{Z}$, the Thue equation $f(x, y) = h$ has at most r rational solutions, provided the Mordell-Weil rank r of the Jacobian of the curve defined by this equation is at most $n - 3$.

Reduction of binary forms — a progress report

M. Stoll

We present some new results related to the reduction theory of binary forms. In particular, we give a lower bound on the size of a form, depending on the distance of its 'Hermite point' from the base point j of hyperbolic space. This leads to an algorithm that solves the following problem.

Given $F \in \mathbf{Z}[X, Y]$ homogeneous of degree n and squarefree, find $\gamma \in \mathrm{SL}_2(\mathbf{Z})$ such that $\|F \cdot \gamma\|$ is smallest, where $\|F\|$ denotes the sum of the squares of the coefficients of F.

Legendre elliptic curves over finite fields

J. Top

(joint work with Roland Auer)

The lecture explained a naive approach towards the problem of finding genus 3 curves C over any given finite field $\mathbf{F}_q$ of odd characteristic, with a number of rational points close to the Hasse-Weil-Serre upper bound $q + 1 + 3[2\sqrt{q}]$.

The idea is to take the curves C_λ, given by the equation

$$x^4 + y^4 + z^4 = (\lambda + 1)(x^2y^2 + y^2z^2 + z^2x^2),$$

and the elliptic curves E_λ given by

$$y^2 = x(x - 1)(x - \lambda)$$

and E'_λ given by

$$(\lambda + 3)y^2 = x(x - 1)(x - \lambda).$$

Then $\#C_\lambda(\mathbf{F}_q) = q + 1 - 3(q + 1 - \#E'_\lambda(\mathbf{F}_q))$, hence the problem boils down to showing that λ exists such that E'_λ has many points.

This is solved for E_λ in general, but unfortunately for E'_λ only when the characteristic is 3.

Cubic forms, quadratic forms, and quadratic rings

D. B. Zagier

The goal of this mostly expository talk, complementary to that of K. Belabas, was to present some of the beautiful properties of binary cubic forms.

1. Class numbers of binary cubic forms

Write $F = [a, b, c, d]$ to denote the form $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ and let $\mathcal{C}$ and $\mathcal{C}^*$ denote the 4-dimensional lattices of forms with (a, b, c, d) in $\mathbf{Z}^4$ or $\mathbf{Z} \times 3\mathbf{Z} \times 3\mathbf{Z} \times \mathbf{Z}$, respectively. We have on $\mathcal{C}$ and $\mathcal{C}^*$ discriminant functions Δ and $D = -\Delta/27$ given by $\Delta([a, b, c, d]) = 18abcd - 4ac^3 - 4b^3d + b^2c^2 - 27a^2d^2$, $D([a, 3b, 3c, d]) = a^2d^2 - 3b^2c^2 + 4ac^3 + 4b^3d - 6abcd$, both invariant w.r.t. the natural action $F \mapsto F \circ \gamma$ of the group $\Gamma = \mathrm{SL}_2(\mathbf{Z})$. The class numbers $H_3(n)$ and $H_3^*(n)$ are defined as the numbers of Γ-equivalence classes of F in $\mathcal{C}$ or $\mathcal{C}^*$ with $\Delta(F) = n$ or $D(F) = n$, respectively, counted with multiplicity $1/|\Gamma_F|$ in the rare cases when $\Gamma_F \neq \{1\}$ (possible only when n or $-3n$ is a square, in which case $|\Gamma_F|$ can be 3). It was shown by Shintani 30 years ago that each of the four Dirichlet series $Z_\pm(s) = \sum_{n>0} H_3(\pm n)\, n^{-s}$, $Z_\pm^*(s) = \sum_{n>0} H_3^*(\pm n)\, n^{-s}$ has a meromorphic continuation and functional equation, but it was only relatively recently that Ohno discovered experimentally, and Nakagawa proved, that only two of these four are essentially different: $H^*(n)$ equals $H(n)$ if $n < 0$ and $3H(n)$ if $n > 0$.

2. Relation to binary quadratic forms

Denote by $\mathcal{Q}$ the lattice of binary quadratic forms $Q = [A, B, C] = Ax^2 + Bxy + Cy^2$ with A, B, $C \in \mathbf{Z}$ and discriminant function $D(Q) = B^2 - 4AC$. There is a Γ-equivariant map (essentially the Hessian) $\mathcal{C}^* \to \mathcal{Q}$ which assigns to a cubic form $F = [a, 3b, 3c, d]$ the quadratic form $q_F = [b^2 - ac, bc - ad, c^2 - bd]$ with the same discriminant. If we write this as $n\,Q$ with $n \in \mathbf{N}$ and $Q \in \mathcal{Q}$ primitive, we obtain a decomposition of $H_3^*(D)$ as $\sum_{d^2|n} H_3^*(D/n^2, n)$. A result going back essentially to Eisenstein (1844) is that for $n = 1$ (the only case that arises if D is fundamental, the case he treated) one has $H_3^*(D, 1) = [U_D : U_D^3] \cdot |\mathrm{Cl}_D[3]|$, where U_D and Cl_D denote the unit and class group of the order $\mathcal{O}_D = \mathbf{Z} + \mathbf{Z}(D + \sqrt{D})/2$ of discriminant D. The description in the general case turns out to be equally simple: $H_3(D, n)$ is equal to the cardinality of $\{(\mathfrak{a}, \theta)\}/\sim$, where $\mathfrak{a}$ runs over invertible (fractional) $\mathcal{O}_D$-ideals and θ over elements in $\mathfrak{a}^3$ with $N(\theta) = nN(\mathfrak{a})^3$ and the equivalence is $(\mathfrak{a}, \theta) \sim (\lambda\mathfrak{a}, \lambda^3\theta)$ for $\lambda \in \mathbf{Q}(\sqrt{D})^\times$. Equivalently, $H_3(D, n)$ equals $H_3(D, 1)$ times the number of integral $\mathcal{O}_D$-ideals of norm n whose class in Cl_D is a perfect cube.

3. Relation to cubic rings

A *cubic ring* is a commutative, associative ring with 1 whose underlying additive group is isomorphic to $\mathbf{Z}^3$. It is an old result, due to Delone and Faddeev, that there is a canonical bijection between isomorphism classes of such rings and $\mathrm{GL}_2(\mathbf{Z})$-equivalence classes of cubic forms (now in $\mathcal{C}$, not $\mathcal{C}^*$). The original construction is highly basis dependent: one chooses a $\mathbf{Z}$-basis $\{e_0, e_1, 1\}$ of a given cubic ring R, defines 9 integers $a, \ldots, \zeta$ by writing e_0^2, e_0e_1 and e_1^2 as $(b, -a, \xi)$, $(s, -r, \eta)$ and $(d, -c, \zeta)$ with respect to this basis, and then checks that the $\mathrm{GL}_2(\mathbf{Z})$-equivalence class of the form $[a, b + 2r, c + 2s, d]$ is independent of the chosen basis, while conversely any choice of 9 integers $a, \ldots, \zeta$, subject to the three conditions $\xi = r^2 + br - as - ac$, $\eta = rs - ad$, $\zeta = s^2 - dr + cs - bd$, leads by the above multiplication formulas to a cubic ring structure on $\mathbf{Z}^3$. The construction can be made somewhat more transparent by choosing a special ("good") basis with $r = s = 0$ (i.e., $e_0e_1 \in \mathbf{Z}$), but remains quite computational. A simpler and completely canonical construction was presented which in the "$R \to [F]$" direction associates to a cubic ring R

the cubic form $F : M \to \Lambda^3(R) \simeq \mathbf{Z}$ on the 2-dimensional lattice $M := R/(\mathbf{Z}\cdot 1)$ defined by $F(\bar{x}) = x^2 \wedge x \wedge 1$, where $x \in R$ is any pre-image of $\bar{x} \in M$.

Edited by Richard Groenewegen, Leiden

Participants

Prof. Dr. Bill Allombert
allomber@math.u-bordeaux.fr
Laboratoire A2X
UFR de Math. et Informatique
Universite Bordeaux I
351, cours de la Liberation
F-33405 Talence Cedex

Prof. Dr. Karim Belabas
Karim.Belabas@math.u-psud.fr
Mathematiques
Universite Paris Sud (Paris XI)
Centre d'Orsay, Batiment 425
F-91405 Orsay Cedex

Prof. Dr. Daniel J. Bernstein
djb@cr.yp.to
Department of Mathematics
University of Illinois at Chicago
M/C 249, 322 SEO
851 S. Morgan Street
Chicago IL-60607-7045
USA

Prof. Dr. Frits Beukers
beukers@math.ruu.nl
Mathematisch Instituut
Universiteit Utrecht
P. O. Box 80.010
NL-3508 TA Utrecht

Prof. Dr. Bryan J. Birch
birch@maths.oxford.ac.uk
Mathematical Institute
Oxford University
24 - 29, St. Giles
GB-Oxford OX1 3LB

Wieb Bosma
bosma@sci.kun.nl
Mathematisch Instituut
Katholieke Universiteit Nijmegen
Toernooiveld 1
NL-6525 ED Nijmegen

Prof. Dr. Nils Bruin
bruin@cecm.sfu.ca
Dept. of Mathematics and Statistics
Simon Fraser University
Burnaby 2, B.C. V5A 1S6
CANADA

Prof. Dr. Armand Brumer
brumer@fordham.edu
Department of Mathematics
Fordham University
Bronx, NY 10458
USA

Dr. Dongho Byeon
dhbyeon@kias.re.kr
School of Mathematics
Korea Inst. for Advanced Study
207-43 Cheongryangri-dong,
Dondaemun-gu
Seoul 130-012
KOREA

Prof. Dr. Henri Cohen
cohen@math.u-bordeaux.fr
Laboratoire A2X
UFR de Math. et Informatique
Universite Bordeaux I
351, cours de la Liberation
F-33405 Talence Cedex

Prof. Dr. Jean-Marc Couveignes
couveig@univ-tlse2.fr
GRIMM, UFR SES
Universite Toulouse II
5, Allee Antonio Machado
F-31058 Toulouse

Johnny Edwards
edwards@math.uu.nl
Magdalenastraat 28
NL-3512 NH Utrecht

Prof. Dr. Noam D. Elkies
elkies@math.harvard.edu
Dept. of Mathematics
Harvard University
1 Oxford Street
Cambridge, MA 02138
USA

Dr. Claus Fieker
claus@maths.usyd.edu.au
School of Mathematics & Statistics
University of Sydney
Sydney NSW 2006
AUSTRALIA

Prof. Dr. David Ford
ford@mathstat.concordia.ca
Department of Computer Science
Concordia University
1455 de Maisonneuve Blvd. West
Montreal Quebec H3G 1M8
CANADA

Prof. Dr. Gerhard Frey
frey@exp-math.uni-essen.de
Institut für Experimentelle
Mathematik
Universität-Gesamthochschule Essen
Ellernstr. 29
45326 Essen

Eduardo Friedman
friedman@uchile.cl
Depto. Matematicas
Universidad de Chile
Casilla 653
Santiago
CHILE

Dr. Herbert Gangl
herbert@mpim-bonn.mpg.de
Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn

Dr. Martine Girard
girard@math.leidenuniv.nl
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Prof. Dr. Richard P. Groenewegen
groen@math.leidenuniv.nl
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Prof. Dr. Paul E. Gunnells
gunnells@math.columbia.edu
Department of Mathematics
Rutgers University
Newark, NJ 07102
USA

Prof. Dr. Michael John Jacobson
jacobs@cs.umanitoba.ca
Department of Computer Science
The University of Manitoba
Winnipeg, Manitoba R3T 2N2
CANADA

Dr. Jürgen Klüners
klueners@iwr.uni-heidelberg.de
Interdisziplinäres Zentrum
für Wissenschaftliches Rechnen
Universität Heidelberg
Im Neuenheimer Feld 368
69120 Heidelberg

David Kohel
kohel@math.usyd.edu.au
School of Mathematics & Statistics
University of Sydney
Sydney NSW 2006
AUSTRALIA

Prof. Dr. Emmanuel Kowalski
emmanuel.kowalski@math.u-bordeaux.fr
Laboratoire A2X
UFR de Math. et Informatique
Universite Bordeaux I
351, cours de la Liberation
F-33405 Talence Cedex

Dr. Franz Lemmermeyer
franzl@csusm.edu
California State University at
San Marcos
Department of Mathematics
333 South Twin Oaks Valley Rd.
San Marcos, CA 92096-0001
USA

Prof. Dr. Hendrik W. Lenstra, Jr.
hwl@math.berkeley.edu
Department of Mathematics
University of California
at Berkeley
Berkeley, CA 94720-3840
USA

Prof. Dr. Christian Maire
maire@math.u-bordeaux.fr
Laboratoire A2X
UFR de Math. et Informatique
Universite Bordeaux I
351, cours de la Liberation
F-33405 Talence Cedex

Prof. Dr. Jean-Francois Mestre
mestre@math.jussieu.fr
U. F. R. de Mathematiques
Case 7012
Universite de Paris VII
2, Place Jussieu
F-75251 Paris Cedex 05

Dr. Preda Mihailescu
preda@uni-paderborn.de
FB 17: Mathematik/Informatik
Universität Paderborn
33095 Paderborn

Prof. Dr. Catherine O'Neil
coneil@math.mit.edu
Department of Mathematics
Massachusetts Institute of
Technology
Cambridge, MA 02139-4307
USA

Prof. Dr. Michel Olivier
olivier@math.u-bordeaux.fr
Laboratoire A2X
UFR de Math. et Informatique
Universite Bordeaux I
351, cours de la Liberation
F-33405 Talence Cedex

Prof. Dr. Xavier Roblot
roblot@desargues.univ-lyon1.fr
Institut Girard Desargues
Universite Claude Bernard
43, Bd. du 11 Novembre 1918
F-69622 Villeurbanne Cedex

Prof. Dr. Rene Schoof
schoof@wins.uva.nl
Dipartimento di Matematica
2. Universita di Roma
"TOR VERGATA"
I-00185 Roma

Prof. Dr. Robert Sczech
sczech@andromeda.rutgers.edu
Dept. of Mathematics & Computer Sc.
Rutgers University
101 Warren Street
Newark, NJ 07102
USA

Denis Simon
desimon@math.u-bordeaux.fr
Laboratoire A2X
UFR de Math. et Informatique
Universite Bordeaux I
351, cours de la Liberation
F-33405 Talence Cedex

Dr. Chris J. Smyth
c.smyth@edinburgh.ac.uk
Dept. of Mathematics & Statistics
University of Edinburgh
James Clerk Maxwell Bldg.
King's Building, Mayfield Road
GB-Edinburgh, EH9 3JZ

Prof. Dr. Harold M. Stark
stark@math.ucsd.edu
Dept. of Mathematics
University of California, San Diego
9500 Gilman Drive
La Jolla, CA 92093-0112
USA

Dr. William A. Stein
was@math.berkeley.edu
Dept. of Mathematics
Harvard University
1 Oxford Street
Cambridge, MA 02138
USA

Peter Stevenhagen
psh@math.leidenuniv.nl
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Dr. Michael Stoll
stoll@math.uni-duesseldorf.de und
stoll@mpim-bonn.mpg.de
Mathematisches Institut
Heinrich-Heine-Universität
Gebäude 25.22
Universitätsstraße 1
40225 Düsseldorf

Dr. Jaap Top
j.top@math.rug.nl
Mathematisch Instituut
Rijksuniversiteit Groningen
Postbus 800
NL-9700 AV Groningen

Prof. Dr. Don B. Zagier
zagier@mpim-bonn.mpg.de
Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn

Prof. Dr. Horst Günter Zimmer
zimmer@math.uni-sb.de
Fachbereich 9 - Mathematik
Universität des Saarlandes
Postfach 151150
66041 Saarbrücken