Diophantine Approximation

July 28 - August 2, 2003

List of abstracts

M. Bennett

Rational Torsion Subgroups of Elliptic Curves in Short Weierstrass Form

A recent paper claimed to show that an elliptic curve

$$E : y^2 = x^3 + Ax + B$$

where A and B are nonzero integers with $A > |B| > 0$ has rational torsion subgroup of order $1, 3$ or 9. We will provide a series of counterexamples to this statement and will, in fact, show that, if A is "suitably large", relative to B, then such a curve has only trivial rational torsion. Our proof, perhaps somewhat surprisingly, relies upon Roth's theorem on rational approximation to algebraic numbers.

A. Bérczes (joint work with J.-H. Evertse and K. Győry)

On the number of binary forms with given discriminant and degree

Let S be a finite set of rational primes. Denote by $\mathbb{Z}_S$ the ring of S-integers in $\mathbb{Q}$ and by $\mathbb{Z}_S^*$ its unit group. Two binary forms are called $\mathbb{Z}_S$-equivalent if $F(X,Y) = G(AX + BY, CX + DY)$ with $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in GL(2, \mathbb{Z}_S)$. The discriminants of $\mathbb{Z}_S$-equivalent binary forms differ only by a factor from $\mathbb{Z}_S^*$.

In 1972, Birch and Merriman proved that for given $n \geq 3$ and non-zero $c \in \mathbb{Z}_S$ the number of $\mathbb{Z}_S$-equivalence classes of binary forms $F(X,Y) \in \mathbb{Z}_S[X,Y]$ with

$$D(F) \in c\mathbb{Z}_S^* \tag{1}$$

is finite. In 1991, Evertse and Győry proved an effective version of this result which makes it possible, at least in principle, to determine a full system of representatives of the $\mathbb{Z}_S$-equivalence classes of F satisfying (1).

Recently, we gave an explicit upper bound for the number of $\mathbb{Z}_S$-equivalence classes of irreducible binary forms $F(X,Y) \in \mathbb{Z}_S[X,Y]$ of degree n, satiafying (1) and having a root in a fixed number field. We also obtained a similar result concerning reducible binary forms.

Y. Bilu (joint work with M. Kulkarni and B. Sury)

Erdős-Selfridge translated

Let r be an integer, not a perfect power. Then the equation

$$x(x+1)...(x+m-1)+r=y^n$$

has finitely many integer solutions (x,y,m,n) (with $m,n>1$), and all solutions can be effectively determined.

A. Biro (joint work with A. Granville)

Zeta functions for ideal classes of real quadratic fields at $s=0$

We give explicit formulas (involving regular continued fraction expansions) in general real quadratic fields for the special values mentioned in the title. In the case of some special quadratic fields the previously proved special cases of these formulas were important in the solution of the class number one problems (Yokoi's and Chowla's conjecture) for those fields.

W. D. Brownawell

Independence over Function Fields

This talk will describe some of the recent advances in independence for function fields over $k=\mathbb{F}_q(t)$ and compare and contrast the situation with the classical one.
In work to appear, G.W. Anderson, M. Papanikolas, and I have shown that all $\overline{k}$-linear relations on monomials in the special Gamma values $\Gamma(a/f)$ are spanned by the relations on pairs of monomials. These relations on pairs are the precise analogues for Thakur's function field Gamma function of the Deligne-Koblitz-Ogus relations for the classical Gamma values. Our proven knowledge about algebraic relations in the classical situation is much more modest.
I will illustrate our new independence criterion for periods of dual t-motives by reproving Wade's result on the transcendence of the Carlitz period.
Then I will illustrate the progress (ongoing joint work with Papanikolas) toward the function field version of "Shimura's Conjecture" by exhibiting the values $\Gamma(a/T(T+1))$, $a\in\mathbb{F}_3[T]$ in terms of periods (and quasi-periods) of Carlitz modules over appropriate rings. This expression will make the "Deligne-Koblitz-Ogus" relations on the Gamma values evident.

N. Bruin

Smooth plane quartics and the arithmetic of their Prym varieties

In this talk, we will consider smooth projective plane quartics of the form

$$C : Q_0(Q_1(x, y, z), Q_2(x, y, z), Q_3(x, y, z)) = 0,$$

where Q_0, Q_1, Q_2, Q_3 are all quadratic forms. In fact, any smooth plane quartic can be written in this form over a sufficiently large field.
Such quartics admit an unramified double cover by a curve D of genus 5, which in turn can be mapped into an Abelian surface - the Prym-variety of the cover D over C. All of these objects can be made completely explicit and are quite accessible to computation. This allows the application of explicit Chabauty-techniques to the embedding of D in the Prym-variety.
Because the embedding of D in the Prym is independent of the existence of a rational point or a degree-1 divisor class on D, this configuration allows for easy, non-trivial computations in the Brauer-Manin obstruction of D.
The Brauer-Manin obstruction is an attempt to generalise the concept of local obstructions to rational points on varieties. Indeed, we will give an example of an everywhere locally solvable curve D which has no rational points.

Y. Bugeaud

Exponents of Diophantine approximation.

According to Mahler and Koksma, for any positive integer n and any real number ξ, we denote by $w_n(\xi)$ (resp. by $w_n^*(\xi)$) the supremum of the real numbers w such that, for infinitely many integers H, the equation

$$0 < |P(\xi)| < H^{-w} \qquad \text{resp. } 0 < |\xi - \alpha| < H^{-w-1}$$

is satisfied with an integer polynomials $P(X)$ (resp. in real algebraic numbers α) of degree at most n and height at most H. We define the exponents of approximation $\hat{w}_n(\xi)$ and $\hat{w}_n^*(\xi)$ by replacing 'for infinitely many integers H' by 'for all integers H large enough' in the above definition. Taking also into account the simultaneous approximation of $\xi, \ldots, \xi^n$ by rationals, we thus introduce four new exponents of approximation attached to ξ. We survey the known relationships between them and we discuss some open questions.

P. Bundschuh (joint work with V.G. Chirskii (Moscow))

Algebraic independence of elements from $\mathbb{C}_p$ over $\mathbb{Q}_p$

The question in the title has been studied in the past only occasionally. For a brief survey on what was published on this topic so far, we refer to our joint paper [Arch.Math. 79, 345-352 (2002)]. The main result in this paper provided sufficient conditions for the algebraic independence over $\mathbb{Q}_p$ of elements from $\mathbb{C}_p$ defined by infinite series of the form $\sum a_k p^{r_k}$, where (r_k) is a sequence of positive rational numbers and the a_k are p-adic integers.
In our recent work we shall propose two new criteria, where the hypotheses on the a_k, r_k are now slightly stronger. But, on the other hand, we need not longer, as in our paper quoted above, conditions on determinants involving certain of the coefficients a occurring in the different series under consideration.
Both of our new criteria have the same typical appearance: Under appropriate assumptions on functions $f_1, ..., f_\ell$ and points $\alpha_1, ..., \alpha_m$, the $\ell \cdot m$ elements $f_\lambda(\alpha_\mu)$ from $\mathbb{C}_p$ are algebraically independent over $\mathbb{Q}_p$.

P. Corvaja (Joint work with U. Zannier)

On a generalization of the Subspace Theorem and a generalization of Thue equations.

We provide a lower bound for the product of values polynomials (satisfying suitable conditions) at integral points. As a corollary, we obtain degeneracy and finiteness results for integral points on varieties defined by equations of the type $f_1(x_1, \ldots, x_n) \cdots f_r(x_1, ldots, x_n) = g(x_1, \ldots, x_n)$, where $f_1, \ldots, f_r, g$ are polynomials and g has "small" degree.

S. David

On the height of points on subvarieties of multiplicative groups

We shall discuss conjectures and recent results on the last non trivial minimum for the height of points on subvarieties of multiplicative groups.

C. Fuchs

Diophantine inequalities involving several power sums

Let $\mathcal{E}_A$ denote the ring of power sums, i.e. complex functions on $\mathbb{N}$ of the form

$$G_n = c_1\alpha_1^n + c_2\alpha_2^n + \cdots + c_t\alpha_t^n,$$

for some $c_i \in \mathbb{C}$ and $\alpha_i \in A$, where $A \subset \mathbb{C}$ is multiplicative semigroup. It is well known that such functions satisfy linear recurrence relations

$$G_n = A_1 G_{n-1} + \cdots + A_k G_{n-k} \quad \text{for} \quad n = k, k+1, \ldots$$

with constant coefficients, where the α_i are roots of the corresponding characteristic polynomial

$$X^k - A_1 X^{k-1} - \cdots - A_k,$$

the general solutions being of the same form, but allowing the c_i to be polynomials in n.

Recently, many Diophantine problems involving power sums were considered by using deep tools from Diophantine approximation (especially Schmidt's Subspace Theorem), e.g. by Corvaja and Zannier.

In this talk we will first give a survey on recent developments on such problems and then present new results (jointly with A. Scremin): Let $F(n, y) \in \mathcal{E}_{\mathbb{N}}[y]$ and $\epsilon > 0$. We consider Diophantine inequalities of the form

$$\Big| F(n, y) \Big| = \Big| f(G_n^{(1)}, \ldots, G_n^{(d)}, y) \Big| < \alpha^{n(d-1-\epsilon)},$$

and show, under suitable conditions, that all the solutions $(n, y) \in \mathbb{N} \times \mathbb{Z}$ have y parametrized by some power sums from a finite set, where

$$\alpha = \max_{i=1,\ldots,d} \left(\alpha_1^{(i)} \right)^{\frac{1}{i}}.$$

This is a continuation of the work of Corvaja and Zannier and of Scremin and the speaker on such problems.

K. Győry

On the Diophantine equation $1^k + \ldots + x^k = y^n$

The title equation and its various generalizations were studied by many people, including Lucas, Schaffer, Tijdeman, Voorhoeve, Gyory, Brindza, Dilcher, Urbanowicz, Pinter and Walsh. They have established general finiteness theorems, as well as some upper bounds on n and the number of solutions. In the first part of our talk we give a survey on these results.

In the second part, some new results obtained jointly with M.Bennett and A.Pinter will be presented.The main result is that apart from some trivial (and well-known) solutions, the title equation has no solution in x, y and n if $k \leq 11$. Our proof requires a combination of virtually every technique in modern Diophantine analysis, including local methods, a classical reciprocity theorem in cyclotomic fields, lower bounds for linear forms in logarithms of algebraic numbers and in elliptic logarithms, a computational method for finding the solutions to elliptic equations, the hypergeometric method of Thue and Siegel and results on ternary equations based upon Galois representations and modular forms. It is a rare situation where one can explicitly solve superelliptic equations of as high degree as we encountered in our proof. This was accomplished by solving certain high degree Thue equations, itself being a notoriously difficult problem.

L. Hajdu

Almost perfect powers in products of consecutive terms from an arithmetic progression (joint work with M. Bennett, K. Győry and N. Saradha)

We consider the diophantine equation

$$n(n+d)...(n+(k-1)d) = by^l \tag{2}$$

in positive integers n, d, k, b, y, l with $k, l \geq 2$, $\gcd(n, d) = 1$ and $P(b) \leq k$. Here $P(u)$ stands for the greatest prime factor of u if $u > 1$ is an integer, and we put $P(1) = 1$.

Equation (2) and its various generalizations have been considered by several mathematicians, e.g. by Euler, Erdős, Selfridge, Shorey, Tijdeman, Saradha, Győry and Bennett. Euler proved that the product of four consecutive terms from an arithmetic progression is never a perfect square.

By a famous result of Erdős and Selfridge, the product of two or more consecutive integers is never a perfect power. These results concern the case when in equation (1) we have $b = d = 1$. They were extended by Saradha (case $k \geq 4$) and Győry (case $k = 2, 3$) to the case when $d = 1$, but b is not necessarily 1.
The general situation when $d > 1$ is more complicated. Though equation (1) has attracted the attention of several mathematicians, only some partial results are known so far. One of the most interesting results, due to Shorey and Tijdeman, asserts that for any l, in (2) k can be bounded in terms of $\omega(d)$, the number of prime divisors of d.

In the talk I present some new results obtained jointly with *M. Bennett, K. Győry* and *N. Saradha*. Together with Győry and Saradha we proved that for fixed $k \geq 3$ and $l \geq 2$ with $k + l > 6$, equation (2) has only finitely many solutions in n, d, b, y. Jointly with Bennett and Győry we showed that if $k \geq 4$ is fixed, then under certain technical assumptions (2) has at most finitely many solutions in n, d, b, y, l with $P(b) < k/2$.
For small values of k, we showed that for $3 \leq k \leq 11$, the product of k consecutive terms from a positive arithmetic progression is never a perfect power. For $k = 3$, this is due to Győry, for $k = 4, 5$ to Győry, Hajdu and Saradha and for $6 \leq k \leq 11$ to Bennett, Győry and Hajdu, respectively. In fact we proved with Bennett and Győry a more general version of this theorem when n is a non-zero integer, $b \geq 1$ and $P(b) < \max(3, k/2)$.
In the proofs of our theorems we used sevaral classical and modern results and methods from Diophantine analysis, such as Galois representations, Frey curves and modular forms.

N. Hirata-Kohno

Linear forms in p-adic elliptic logarithms

We talk about a lower bound for linear forms in p-adic elliptic logarithms. Let $\mathcal{E}$ be an elliptic curve defined over a number field K. A usual elliptic logarithm is defined as $u \in \mathbf{C}$ such that $\exp(u) \in \mathcal{E}(\mathcal{K})$. Now let p be a rational prime and v be a place of K over p. Consider K_v a completion of K by v. Let $u \in K_v$ (not $\mathbf{C}$) satisfying $\exp(u) \in \mathcal{E}(\mathcal{K})$, which is called p-adic elliptic logarithm. We give here an explicit lower bound for a p-adic absolute value of a linear combination of such p-adic elliptic logarithms in rational case.

I. Járási

Computing the small solutions of unit equations with an application to resultant form equations.

This talk is a completion of the speakers talk of the last years Diophantine Workshop in Leiden. We construct an algorithm to enumerate small solutions of unit equations in three variables. The algorithm is a generalization of Wildanger's method and of the method of Gaal and Pohst, and is based on the method of Fincke and Pohst enumerating lattice points in ellipsoids. An application of the method to compute the small solutions of special resultant form equations will also be presented. In this talk mostly the problems of the specific examples and the possible generalizations will be concerned. Also numerical examples wil be given.

M. Laurent

Diophantine properties of Sturmian type numbers.

We call sturmian a real number ξ whose sequence of partial quotients is given by a Sturm word in two letters a and b replaced by distinct positive integers. It is known that such a number ξ has a lot of quadratic approximations ensuring that it is transcendental. We compute explicitely in term of the Sturm sequence various measures of diophantine approximation of ξ, including measures of quadraticity, measure of simultaneous rational approximation of $\xi, \xi^2, \ldots$
Our results extend to general sturmian sequences recent works of Damien Roy in the special case of the Fibonacci word.

Y. Nesterenko

Multiplicity estimates and transcendence theory

We will give a survey of multiplicity estimates beginning with the results of Rob Tijdeman.

R.Okazaki

A sharp upper bound on the numbers of solutions of certain quartic Thue equations.

Let $f(X,Y)$ be a binary quartic form with integer coefficients. We assume $f(X,1) = 0$ has four distinct real roots. Then, the number of solutions to the Thue equation $|f(X,Y)| = 1$ is at most 12 if the disciminant of $f(X,Y)$ is larger than a constant C. A suitable value of C is under calculation.

P. Olajos

Recent results on power integral bases of composite fields.

We consider the problem of existence of power integral bases in orders of composite fields. Completing our former results we show that under certain congruence conditions on the coefficients of the defining polynomial of the generating elements of the fields, the composite of the polynomial orders does not admit power integral basis. As applications we provide several examples.

A. Pethö

Application of decomposable form functions in cryptography

In the talk I will give an overview on recent investigations of the cryptography group at the University of Debrecen.

Let $R(X) \in \mathbb{Z}[X]$ be monic and without multiple roots and denote by $\mathcal{N}_R(\underline{X})$ the norm form associated to $R(X)$. Let p, q be primes such that $p < q < 2p$ and put $s = pq$. Bérczes and Ködmön proved that the value $\mathcal{N}_R(\underline{x})$ and $\mathcal{N}_{R,s}(\underline{x}) = \mathcal{N}_R(\underline{x}) \bmod s$ at the point $\underline{x} \in \mathbb{Z}^n$ can be computed efficiently. With the same colleagues we showed that $\mathcal{N}_{R,s}(\underline{x})$ is collision resistant, i.e. it can be used as a hash function. We found also some fact, which show that $\mathcal{N}_{R,s}(\underline{x})$ is probably a family of one way functions.

A.J. van der Poorten

Continued fractions and multiples of a point on an elliptic curve

The continued fraction expansion of the square root of a generic quartic polynomial provides parameters detailing the multiples of a nominated point on an elliptic curve and readily yields such objects as raw forms for the modular curves $X_1(m)$, elliptic divisibility sequences, and related wonders.

C. Rakaczki

On the diophantine equation $F\left(\binom{x}{n}\right) = b\binom{y}{m}$.

The title equation has been studied by many people in various special cases. Several results have been obtained which state that under certain conditions on F, b, m, and n, the equation has only finitely many solutions in x, y. In our talk we present the following generalization. Let $F(x) \in \mathbb{Z}[x]$ be a polynomial of degree 1 or p, where p is a prime. Further let $b \neq 0$ be an integer. We characterize those pairs $(m, n) \in \mathbb{N}^2$ and polynomials $F(x)$ for which the title equation has only finitely many integer solutions $x \geq n$, $y \geq m$.

G. Rémond

Intersecting curves and algebraic groups.

Following a result of Bombieri, Masser and Zannier on tori, E. Viada proved that the intersection of a curve C in power E^g of a C. M. elliptic curve with the union of all algebraic subgroups of E^g of codimension 2 is a finite set, provided that C is not contained in any translate of an algebraic subgroup of codimension 1. In this talk I explain that this is still true if one assume only that C is not contained in any algebraic subgroup of codimension 1. This is stronger than it may appear because the new statement implies Mordell's conjecture. Accordingly, the proof uses a modification of the argument of Vojta for Mordell's conjecture. I also discuss what can be said when E^g is replaced by an arbitrary abelian variety A and a partial result of "Mordell-Lang plus Bogomolov" type.

T. Rivoal

Multiple integrals and multipolylogarithms

A survey about zeta function values, and their extension to multi zeta values

D. Roy

Approximation to real numbers by cubic algebraic integers

It has been conjectured for some time that, for any integer $n \geq 2$, any real number $\epsilon > 0$ and any transcendental real number ξ, there would exist infinitely many algebraic integers α of degree at most n with the property that $|\xi - \alpha| \leq H(\alpha)^{-n+\epsilon}$, where $H(\alpha)$ denotes the height of α. Although this is true for $n = 2$, we show in this talk that, for $n = 3$, the optimal exponent of approximation is not 3 but $(3 + \sqrt{5})/2 \simeq 2.618$.

M. Ru

Diophantine approximation and Nevanlinna theory

In this talk, I'll first briefly describe the interconnections between Diophantine approximation and Nevanlinna theory, discovered by Osgood, Vojta, Lang and others. Then, I plan to give a survey of recent results on the extension of Schmidt's subspace theorem, moving target problems, as well as the uniqueness theorems.

A. Schinzel (joint work with I. Aliev and W. M. Schmidt)

On vectors whose span contains a given linear subspace

Let for $k > l > m > 0$

$$c(k, l, m) = \sup \inf H(S)^{\frac{l-k}{k-m}} \prod_{i=1}^{l} |\mathbf{p}_i| \,,$$

where the supremum is taken over all rational subspaces S of $\mathbb{R}^k$ of dimension m and the infimum is taken over all sets of linearly independent vectors $\mathbf{p}_1, \ldots, \mathbf{p}_l$ in $\mathbb{Z}^k$, whose span contains S. Here $H(S)$ is the determinant of the lattice $S \cap \mathbb{Z}^k$ and $|\mathbf{p}|$ is the Euclidean norm of $\mathbf{p}$. The following theorems hold

Theorem 1.

$$\gamma_{k-m,k-l}^{1/2} \leq c(k,l,m) \leq \gamma_{k-m,k-l}^{1/2} \gamma_l^{1/2}$$

where $\gamma_{r,s}$ is the Rankin constant generalizing Hermite's constant $\gamma_r = \gamma_{r,1}$.

Theorem 2.

$$c(3,2,1) \geq 6/\sqrt[4]{722}.$$

W.M. Schmidt

Covering and Packing in $\mathbb{Z}^n$ and $\mathbb{R}^n$

Symposium lecture

T. Shorey

A conjecture of Erdős on powers in products of integers in arithmetic progression.

A well-known theorem of Euler states that a product of four terms in an arithmetic progression is never a square. I shall give several extensions of this result.

V. Sós

Interaction between number theory and combinatorics

Symposium lecture

C. Stewart

On integers composed of small primes

Symposium lecture

M. Waldschmidt

Tijdeman's mathematical contributions related to transcendental numbers

Symposium lecture

K. Yu

New progress in the theory of p-adic logarithmic forms

We shall report some new progress in this area after 1999

W. Zudilin (joint with T. Matalo-Aho and K. Väänänen)

New irrationality measures for q-logarithms

We present new sharp upper bounds for irrationality measures of the values of the q-logarithm function

$$\ln_q(1-z) = \sum_{\nu=1}^{\infty} \frac{z^\nu q^\nu}{1-q^\nu}, \qquad |z| \leq 1,$$

when $p = 1/q \in \mathbb{Z}\setminus\{0, \pm 1\}$ and $z \in \mathbb{Q}$. In order to improve the earlier results we shall combine the following three major methods used in diophantine analysis of q-series:

(1) a general hypergeometric construction of rational approximations to the values of q-logarithms vsṫhe q-arithmetic approach;

(2) a continuous iteration procedure for additional optimization of analytic estimates;

(3) introducing the cyclotomic polynomials for sharpening least common multiples of the constructed linear forms in the case when z is a root of unity.

We underline that in the corresponding arithmetic study of the values of the ordinary logarithm (cfṘukhadze's results for log 2 and Hata's estimates for other logarithms) only feature (1) is applied: features (2) and (3) have no ordinary analogues. Thus the present q-problems invoke new attractions in arithmetic questions.