Mathematisches Forschungsinstitut Oberwolfach

Report No. 21/2007

Diophantische Approximationen

Organised by
Yuri V. Nesterenko (Moscow)
Hans-Peter Schlickewei (Marburg)

April 15th – April 21st, 2007

Abstract. This Number Theoretic conference was focused on the following subjects: the Subspace Theorem and its ramifications and applications, heights of subvarieties of group varieties, effective methods for solution of diophantine equations, geometry of numbers, arithmetic properties of zeta-values and other numbers.

Mathematics Subject Classification (2000): 11-06.

Introduction by the Organisers

The workshop Diophantische Approximationen (Diophantine approximations), organised by Yuri V. Nesterenko (Moscow) and Hans-Peter Schlickewei (Marburg) was held April 15th - April 21st, 2007. This meeting was well attended with over 40 participants with broad geographic representation. This workshop was a nice blend of researchers with various backgrounds. All the participants were inspired by the fact that the conference immediately followed the 300 anniversary of Euler birth (15.04.1707).

Loosely speaking Diophantine approximation is a branch of Number Theory that can be described as a study of the solvability of inequalities in integers, though this main theme of the subject is often unbelievably generalized. As an example, one can be interested in properties of rational points of algebraic varieties defined over an algebraic number field. The conference was concerned with a variety of problems of this kind. Below we briefly recall some of the results presented at this conference, thus outlining some modern lines of investigation in Diophantine approximation. More details can be found in the corresponding abstracts.

The classical Subspace Theorem claims that all integer solutions $\mathbf{x} \in \mathbb{Z}^n$ of a special system of linear inequalities with algebraic coefficients belong to a finite number of linear subspaces of $\mathbb{R}^n$. This theorem proved by W.Schmidt in 70-th of 20-th century is a far reaching generalization of the famous theorem of Roth

about approximation of algebraic numbers by rationals. Subsequently Schmidt gave an estimate for the number of such subspaces. This result was improved and extended by H.P. Schlickewei and J.H. Evertse. Another approach to the proof of Schmidt's theorem was proposed by G. Faltings and G. Wüstholz. In the joint talk of J.H. Evertse and R. Ferretti the upper bound for the number of the subspaces in question was significantly improved by combining ideas of Schmidt, Faltings and Wüstholz.

Results of this kind have many applications. For example Y. Bugeaud in his talk announced joint with J.H. Evertse theorem that for any real algebraic number ξ and any integer $b > 1$ the number of distinct blocks of n letters occurring in the b-ary expansion of ξ asymptotically exceed $n(\log n)^\eta$ for any positive $\eta < 1/14$. Another example is connected to the classical theorem of Siegel about integer points on curves of genus $g \geq 1$. In the survey talk of Yu. Bilu another proof of this theorem based on quantitative version of Subspace Theorem was presented. This proof belongs to P. Corvaja and U. Zannier (2002) who applied their arguments to integral points on surfaces. Corresponding results were presented in the talk of Bilu the same as more precise statement of A. Levin and P. Autissier.

Talks of P. Habegger, A. Galateau were devoted to the problem of lower bounds of heights on subvarieties of group varieties that is analogous to the classical Lehmer problem. Earlier works in this direction belong to E. Bombieri, D. Masser, U. Zannier, F. Amoroso, S. David and P. Philippon.

P. Mihailescu discussed in his talk so called Fermat-Catalan equation. In particular he gave some sufficient conditions on prime numbers p, q providing existence only trivial rational solutions for the equation $x^p + y^q = 1$. The methods used by Mihailescu have a cyclotomic nature and they combine class field conditions with some new approximation techniques.

The well-known Khintchine Transference Principle relates the measure of simultaneous rational approximation of the real numbers $\theta_1, \ldots, \theta_n$ with the measure of linear independence over $\mathbf{Q}$ of the numbers $1, \theta_1, \ldots, \theta_n$. M. Laurent introduced in his talk exponents which measure the sharping of the approximation to the point $\Theta = (\theta_1, \ldots, \theta_n)$ by rational linear varieties of dimension d for every integer $d, 0 \leq d < n$, and proved some inequalities connecting these exponents. The Khintchine's inequality follows as a special case. Another kind of transference ideas were used in the joint talk of V. Beresnevich and S. Vilani to state some metric Diophantine approximation results. The transference lemma in functional domain directed to applications in multiplicity estimates and algebraic independence theory was reported by P. Philippon.

The determination of the arithmetic nature of values of the Riemann zeta function $\zeta(s)$ at odd values $s \in \mathbf{Z}$, $s > 3$, is one of the most challenging problems in number theory. After Apery's celebrated proof of the irrationality of $\zeta(3)$, it took over twenty years until T. Rivoal proved that there are infinitely many numbers among $\zeta(3), \zeta(5), \zeta(7), \ldots$ that are linearly independent over $\mathbf{Q}$ and W. Zudilin stated that at least one of $\zeta(5), \zeta(7), \zeta(9), \zeta(11)$ is irrational number. The difficulties are connected to constructions of good rational approximations to the

corresponding values of zeta function. All known constructions have a hypergeometric nature. In a joint talk C. Krattenthaler and T. Rivoal gave a survey of recent constructions and explained the proof of so called Denominator conjecture that is based on some identities between a very-well-poised hypergeometric series and a multiple sum due to G. Andrews. Some constructions of approximations to zeta-values with multiple real integrals were discussed in the talk of C. Viola. T. Rivoal presented a new proof of the irrationality of $\zeta(3)$ that uses the expansion of the Hurwitz zeta function in interpolation series of rational functions. Such an interpolation process was first studied by Rene Lagrange in 1935.

The arithmetic properties of values of the Tschakaloff function $T_q(z)$ have been investigated in many works. One of the open problems is to prove linear independence of values of $T_q(z)$ for rational z with different values of the parameter q. In the joint talk of W. Zudilin and K. Väänänen some results of this kind were presented.

In 2005 C. Fuchs and A. Dujella gave a negative answer on the question of Euler about existence of four positive integers with the property that the product of any two of them plus sum of multipliers is a perfect square. In his lecture C. Fuchs discussed analogous question for any four integer numbers. The new result of A. Dujella, A. Filipin and C. Fuchs is the finiteness of the number of quadruples satisfying this condition. Moreover an effective bound for the size of the integers was proved. A. Dujella in his talk discussed another analogous problem: to find a set of positive distinct integers S such that for any pair $x, y \in S$ the number $xy+1$ is a square. The set $S = \{1, 3, 8, 120\}$ was found by Fermat. It is proved that $\#S \leq 5$ and there exists not more than finitely many sets with 5 elements. But no example has ever been found. These problems are connected to lower bounds for linear forms in logarithms of algebraic numbers. Diophantine equations of another type were discussed in the talk of M. Bennett.

B. Adamczewski surveyed some results connected to some problem of Mahler and Mendés France involving tools from automata theory, combinatorics on words and Diophantine approximation.

Another excellent survey of results and open questions connected to Hilbert's tenth problem about universal algorithm for solution of Diophantine equations was given by Yu. Matiyasevich.

Workshop: Diophantische Approximationen

Table of Contents

Abstracts

On the quantitative subspace theorem

Jan-Hendrik Evertse
(joint work with Roberto Ferretti)

Below, we fix some algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, and choose extensions of the absolute values $|\cdot|_p$ ($p \in M_{\mathbb{Q}} = \{\infty\} \cup \{\text{prime numbers}\}$) to $\overline{\mathbb{Q}}$. The norm of $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{C}^n$ is defined by $\|\mathbf{x}\| = \max(|x_1|, \ldots, |x_n|)$. The (inhomogeneous) height $H^*(L)$ of a linear form $L(\mathbf{X}) = \sum_{i=1}^n \alpha_i X_i$ with coefficients in $\overline{\mathbb{Q}}$ is defined to be the absolute (multiplicative) Weil height of the vector $(1, \alpha_1, \ldots, \alpha_n)$. Further we define the field $\mathbb{Q}(L) := \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$.

Let S be a finite subset of $M_{\mathbb{Q}}$, $n \geq 2$ an integer, $\delta > 0$ a real, and for $p \in S$ let $L_{1p}(\mathbf{X}), \ldots, L_{np}(\mathbf{X})$ be linearly independent linear forms from $\overline{\mathbb{Q}}[X_1, \ldots, X_n]$. In general, in the Subspace Theorem one considers inequalities of the shape

$$\prod_{v \in S} \prod_{i=1}^n |L_{ip}(\mathbf{x})|_p \leq \|\mathbf{x}\|^{-\delta} \quad \text{in } \mathbf{x} \in \mathbb{Z}^n .$$

By an elementary combinatorial argument, originating from Mahler, one can reduce this to a finite number of systems of inequalities of the shape

$$|L_{ip}(\mathbf{x})|_p \leq C_p \|\mathbf{x}\|^{c_{ip}} \ (p \in S, \, i = 1, \ldots, n) \quad \text{in } \mathbf{x} \in \mathbb{Z}^n , \tag{1}$$

where the numbers C_p are positive constants, and where $\sum_{p \in S} \sum_{i=1}^n c_{ip} < 0$.

Schmidt [4] was the first to obtain a quantitative version of the Subspace Theorem. After various improvements and extensions, Schlickewei and the author [2] obtained the following refinement.

Put $\varepsilon_\infty = 1$ and $\varepsilon_p = 0$ if p is a prime. Assume that

$$H^*(L_{ip}) \leq H, \ [\mathbb{Q}(L_{ip}) : \mathbb{Q}] \leq D \text{ for } p \in S, \, i = 1, \ldots, n;$$

$$\# \bigcup_{p \in S} \{L_{1p}, \ldots, L_{np}\} \leq R;$$

$$c_{ip} \leq \varepsilon_p \text{ for } p \in S, \, i = 1, \ldots, n; \quad \sum_{p \in S} \sum_{i=1}^n c_{ip} = -\delta \text{ with } 0 < \delta \leq 1;$$

$$\prod_{p \in S} C_p = \Big(\prod_{p \in S} |\det(L_{1p}, \ldots, L_{np})|_p \Big)^{1/n} .$$

Then the set of solutions $\mathbf{x} \in \mathbb{Z}^n$ of (1) with $\|\mathbf{x}\| \geq \max(H, n^{2n/\delta})$ is contained in the union of at most

$$8^{(n+8)^2} \delta^{-n-4} \log(4DR) \log\log(4DR)$$

proper linear subspaces of $\mathbb{Q}^n$.

Throughout this note, we keep the notation and assumptions from above. Then this result can be improved as follows.

Theorem 1. (Ferretti, E.) *(i) The set of solutions* $\mathbf{x} \in \mathbb{Z}^n$ *of (1) with* $\|\mathbf{x}\| \geq \max(H, n^{2n/\delta})$ *is contained in the union of at most*

$$A := 2^{2n}(10n)^{20}\delta^{-3}\log(2\delta^{-1})\log(4DR)\log\log(4DR)$$

proper linear subspaces of $\mathbb{Q}^n$.

(ii) The set of solutions $\mathbf{x} \in \mathbb{Z}^n$ *of (1) with* $\|\mathbf{x}\| < \max(H, n^{2n/\delta})$ *is contained in the union of at most*

$$B := 10^{3n}\delta^{-1}\log(2\delta^{-1})\log\log(4H)$$

proper linear subspaces of $\mathbb{Q}^n$.

In 1994, Faltings and Wüstholz [3] proved the following refinement of the Subspace Theorem, which was in turn an extension of results by Vojta [6] and Schmidt [5]:

There is a unique, effectively determinable proper linear subspace T of $\mathbb{Q}^n$ such that (1) has only finitely many solutions outside T. Furthermore, T can be chosen from a finite collection, which depends only on the linear forms L_{ip} ($p \in S$, $i = 1, \ldots, n$), and is independent of the constants C_p and the exponents c_{ip}.

It seems hopeless to estimate the number of solutions of (1) outside T, but it is possible to prove the following refinement:

Theorem 2. (Ferretti, E.) *There is a sequence of reals* $Q_1 < Q_2 < \cdots < Q_{[A]-1}$ *(where* A *is the quantity from Theorem 1), such that for every solution* $\mathbf{x} \in \mathbb{Z}^n$ *we have either* $\|\mathbf{x}\| < \max(H, n^{2n/\delta})$ *or* $\|\mathbf{x}\| \in [Q_i, Q_i^{1+\delta/2n}]$ *for some* $i \in \{1, \ldots, [A]-1\}$.

Theorem 1 can be deduced by combining Theorem 2 with the following Gap Principle which is based on Lemma 5 of [1].

Gap Principle. *Let* Q *be a real with* $Q \geq 3$. *Then the set of solutions* $\mathbf{x} \in \mathbb{Z}^n$ *of (1) with* $Q \leq \|\mathbf{x}\| \leq Q^{(1+\delta/2n)}$ *is contained in a single proper linear subspace of* $\mathbb{Q}^n$ *if* $Q \geq n^{2n/\delta}$, *and in the union of at most* $10^{2n}\sqrt{2n}$ *proper linear subspaces of* $\mathbb{Q}^n$ *if* $Q < n^{2n/\delta}$.

Schmidt's original proof of the Subspace Theorem depends upon Roth's Lemma and geometry of numbers. His approach was followed by Schlickewei and the author in their proof of the quantitative Subspace Theorem mentioned above. In 1994, Faltings and Wüstholz gave an entirely new proof of the Subspace Theorem, which uses instead of Roth's Lemma the more general Faltings' Product Theorem, but which avoids geometry of numbers. The method of Faltings and Wüstholz lends itself also to a quantification of the Subspace Theorem, but it leads to a

bound much larger than those mentioned above. The hard core of the proofs of our Theorems 1 and 2 is again Schmidt's method, but we combined this with certain ideas of Faltings and Wüstholz; in particular in our Diophantine approximation argument we used the auxiliary polynomial of Faltings and Wüstholz instead of Schmidt's.

We mention here that part (i) of Theorem 1 and Theorem 2 can be generalized to the setting of twisted heights on $\overline{\mathbb{Q}}^n$ like in Theorem 2.1 of [2]; in particular it is possible to obtain an improvement of that Theorem 2.1 similar to part (i) of Theorem 1 mentioned above.

References

[1] J.-H. Evertse, *On the norm form inequality* $|F(\mathbf{x})| \leq h$, Publ. Math. Debrecen **56** (2000), 337–374.

[2] J.-H. Evertse, H.P. Schlickewei, *A quantitative version of the Absolute Subspace Theorem,* J. reine angew. Math. **548** (2002), 21-127.

[3] G. Faltings, G. Wüstholz, *Diophantine approximations on projective spaces,* Invent. math.**116** (1994), 109-138.

[4] W.M. Schmidt, *The subspace theorem in diophantine approximation,* Compos. Math. **96** (1989), 121-173.

[5] W.M. Schmidt, *Vojta's refinement of the Subspace Theorem,* Trans. Amer. Math. Soc. **340** (1993), 705-731.

[6] P. Vojta, *A refinement of Schmidt's Subspace Theorem,* Amer. J. Math. **111** (1989), 489-518.

Around Roth's Theorem

Yann Bugeaud

In 1955, Roth [7] established that, like almost all real numbers (in the sense of the Lebesgue measure), the algebraic irrational numbers cannot be approximated by rationals at an order greater than 2. As pointed out by Mahler in Appendix B of [5], Roth's Theorem suggests the following problem.

Problem. *Let ξ be an irrational, algebraic real number. To find a positive function $q \mapsto \varepsilon(q)$ of the integral variable q, with the property $\lim_{q\to+\infty} \varepsilon(q) = 0$, such that there are at most finitely many distinct rational numbers p/q with positive denominator for which*

$$\left|\xi - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon(q)}}.$$

As written by Mahler, 'the method of Roth does not seem strong enough for solving this problem'; however, a weaker result was found by Cugiani [3] in 1958.

Theorem (Cugiani, 1958). *Let ξ be a real algebraic number of degree d. For an integer $q \geq 16$, set*

$$\varepsilon(q) = 9d\,(\log\log\log q)^{-1/2}.$$

Let $(p_j/q_j)_{j\geq 1}$ be the sequence of reduced rational solutions of

$$\left|\xi - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon(q)}},$$

ordered such that $16 \leq q_1 < q_2 < \dots$ Then either the sequence $(p_j/q_j)_{j\geq 1}$ is finite, or

$$\limsup_{j\to+\infty} \frac{\log q_{j+1}}{\log q_j} = +\infty.$$

The above theorem was subsequently generalized by Cugiani and Mahler [5] to include non-Archimedean valuations, and is now referred to as the Cugiani–Mahler Theorem.

At the end of the 60's, multidimensional extensions of Roth's Theorem were established by W. M. Schmidt [8]. However, no multidimensional analogue of the Cugiani–Mahler Theorem has been published yet. One of our purposes is precisely to establish such a statement, thanks to a new approach for proving the Cugiani–Mahler Theorem.

For a positive real number η and for irrational numbers $\xi_1, \dots, \xi_n$, we say that the positive integer q corresponds to a primitive solution of

$$q \cdot \|q\xi_1\| \cdots \|q\xi_n\| < \eta$$

if, denoting by p_j the nearest integer to $q\xi_j$ for $j = 1, \dots, n$, the $(n+1)$-tuple $(q, p_1, \dots, p_n)$ is primitive, that is, if the greatest common divisor of $q, p_1, \dots, p_n$ is equal to 1.

Theorem 1. *Let n be a positive integer and $\xi_1, \dots, \xi_n$ be real algebraic numbers such that $1, \xi_1, \dots, \xi_n$ are linearly independent over the rationals. Let $\varepsilon : \mathbf{Z}_{\geq 1} \to \mathbf{R}_{>0}$ be a non-increasing function satisfying*

$$\lim_{q\to+\infty} \varepsilon(q) \cdot (\log\log q)^{1/(2n+6)} = +\infty.$$

Let $(q_j)_{j\geq 1}$ be the sequence of positive integers corresponding to primitive solutions of

$$q \cdot \|q\xi_1\| \cdots \|q\xi_n\| < q^{-\varepsilon(q)},$$

ordered such that $1 \leq q_1 < q_2 < \dots$ If this sequence is infinite, then

$$\limsup_{j\to+\infty} \frac{\log q_{j+1}}{\log q_j} = +\infty.$$

Theorem 2. *Let n be a positive integer and ξ be a real algebraic number of degree greater than n. Let $\varepsilon : \mathbf{Z}_{\geq 1} \to \mathbf{R}_{>0}$ be a non-increasing function satisfying*

$$\lim_{H\to+\infty} \varepsilon(H) \cdot (\log\log H)^{1/(2n+6)} = +\infty.$$

Let $(\alpha_j)_{j\geq 1}$ be the sequence of distinct algebraic numbers of degree at most n with

$$|\xi - \alpha| < H(\alpha)^{-n-1-\varepsilon(H(\alpha))},$$

ordered such that $1 \le H(\alpha_1) \le H(\alpha_2) \le \dots$ *Then either this sequence is finite or*

$$\limsup_{j\to+\infty} \frac{\log H(\alpha_{j+1})}{\log H(\alpha_j)} = +\infty.$$

In addition, we would like to point out another important application of our method, dealing with the complexity of irrational, algebraic numbers.

Let $b \ge 2$ be an integer and ξ be a real number with $0 < \xi < 1$. There exists a unique infinite sequence $\mathbf{a} = (a_j)_{j\ge1}$ of integers from $\{0, 1, \dots, b-1\}$, called the b-ary expansion of ξ, such that

$$\xi = \sum_{j\ge1} \frac{a_j}{b^j},$$

and $\mathbf{a}$ does not terminate in an infinite string of 0. For $n \ge 1$, let $p(n, \xi, b) = p(n, \mathbf{a})$ be the number of distinct blocks of n letters occurring in the infinite word $\mathbf{a}$.

Assume from now on that ξ is algebraic and irrational. In 1997, Ferenczi and Mauduit [4] applied a non-Archimedean extension of Roth's Theorem established by Ridout [6] to show that

$$\lim_{n\to+\infty} \big(p(n, \xi, b) - n\big) = +\infty.$$

Then, a new combinatorial transcendence criterion proved with the help of the Schmidt Subspace Theorem by Adamczewski, Bugeaud, and Luca [2] enabled Adamczewski and Bugeaud [1] to establish that

$$\lim_{n\to+\infty} \frac{p(n, \xi, b)}{n} = +\infty.$$

By combining a similar extension of the Cugiani–Mahler Theorem with a careful use of the quantitative Subspace Theorem, in a joint work with Jan-Hendrik Evertse, we are able to improve the above result as follows.

Theorem 3. *Let $b \ge 2$ be an integer and ξ be an algebraic irrational number with $0 < \xi < 1$. Then, for any positive real number η such that $\eta < 1/14$, we have*

$$\lim_{n\to+\infty} \frac{p(n, \xi, b)}{n(\log n)^\eta} = +\infty.$$

References

[1] B. Adamczewski and Y. Bugeaud, *On the complexity of algebraic numbers I. Expansions in integer bases*, Ann. of Math. 165 (2007), 547–565.

[2] B. Adamczewski, Y. Bugeaud et F. Luca, *Sur la complexité des nombres algébriques*, C. R. Acad. Sci. Paris 339 (2004), 11–14.

[3] M. Cugiani, *Sull'approssimazione di numeri algebrici mediante razionali*, Collectanea Mathematica, Pubblicazioni dell'Istituto di matematica dell'Università di Milano 169, Ed. C. Tanburini, Milano, pagg. 5 (1958).

[4] S. Ferenczi and Ch. Mauduit, *Transcendence of numbers with a low complexity expansion*, J. Number Theory 67 (1997), 146–161.

[5] K. Mahler, Lectures on Diophantine approximation, Part 1: g-adic numbers and Roth's theorem, University of Notre Dame, Ann Arbor, 1961.

[6] D. Ridout, *Rational approximations to algebraic numbers*, Mathematika 4 (1957), 125–131.
[7] K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika 2 (1955), 1–20; corrigendum, 168.
[8] W. M. Schmidt, Diophantine Approximation. Lecture Notes in Mathematics 785, Springer, 1980.

Siegel's Theorem on Surfaces (after Levin and Autissier)

Yuri Bilu

We discuss the beautiful theorem of Levin and Autissier: *an affine surface with* 4 *(or more) properly intersecting ample divisors at infinity cannot have a Zariski dense set of integral points.*

1. Integral Points on Curves

Let $\bar{C}$ be an absolutely irreducible projective curve defined over a number field K and let C be an affine subset of $\bar{C}$ embedded into the affine space $\mathbb{A}^\nu$. Further, let S be a finite set of absolute values of K, including all archimedean absolute values, and let $\mathcal{O}_S$ be the ring of S-integers of K. Siegel's classical theorem (in the more general form due to Mahler and Lang) asserts that C has at most finitely many points in $\mathbb{A}^\nu(\mathcal{O}_S)$ if $\mathbf{g}(\bar{C}) \geq 1$ or if $\left|\bar{C} \setminus C\right| \geq 3$.

Of course, one should mention the celebrated result of Faltings, who proved that the set of rational points on a projective curve of genus 2 or higher is finite. We do not discuss Faltings' work here.

The conventional proof of Siegel's theorem relies on the Theorem of Roth[1] and heavily depends on the existence of the Jacobian embedding $\bar{C} \hookrightarrow J(\bar{C})$, because it exploits high degree étale coverings of $\bar{C}$.

Recently Corvaja and Zannier [2] suggested a beautiful new proof, based on the Subspace Theorem of Schmidt and Schlickewei rather than the Theorem of Roth, and using projective rather than Jacobian embeddings.

Corvaja and Zannier prove the following theorem.

Theorem 1.1. *In the above set-up assume that* $\left|\bar{C} \setminus C\right| \geq 3$. *Then* C *has at most finitely many points in* $\mathbb{A}^\nu(\mathcal{O}_S)$.

Siegel's theorem easily follows from Theorem 1.1. Indeed, if $\mathbf{g}(\bar{C}) \geq 1$ then there is an étale covering $\bar{C}' \to \bar{C}$ of degree 3. It induces the covering of affine curves $C' \to C$, and we have $\left|\bar{C}' \setminus C'\right| \geq 3$.

By the Chevalley-Weil principle, the set $\bar{C}(K)$ is covered by $\bar{C}'(K')$, where K' is a number field. Theorem 1.1 implies that the set of $\mathcal{O}_{S'}$-integral points on C' is finite (where S' is the extension of S to K'). Hence so is the set of S-integral points on C.

[1] At the time of Siegel Roth's theorem was not available, and Siegel had to use a weaker statement.

Proof of Theorem 1.1. Write $\bar{C} \setminus C = \{Q_1, \dots, Q_r\}$, where, by the assumption, $r \geq 3$. Extending the field K, we may assume that each of the points $Q_1, \dots, Q_r$ is defined over K. Further, let $D = Q_1 + \dots + Q_r$ be the "divisor at infinity".

Let n be a (big) positive integer, to be specified later. By the Riemann-Roch theorem, the dimension $\ell = \ell(nD)$ of the vector space

$$\mathcal{L} = \mathcal{L}(nD) = \{y \in K(C) : (y) + nD \geq 0\}$$

is given by $\ell = nr - O(1)$. In particular, for big n we have $\ell \sim nr$.

Pick a basis $y_1, \dots, y_\ell$ of $\mathcal{L}$. Multiplying each y_j by a suitable non-zero constant, we may assume that for every S-integral point P we have $y_j(P) \in \mathcal{O}_S$.

Now let $P_1, P_2, P_3, \dots$ be an infinite sequence of distinct S-integral points. Replacing it by a subsequence, we may assume that the sequence (P_i) converges in v-adic topology for every $v \in S$, and we denote by Q_v the corresponding limits. Now we partition our set S as $S = S_0 \cup S_1$, letting S_1 consist of $v \in S$ such that $Q_v \in \bar{C} \setminus C$ and S_0 of those v for which $Q_v \in C$. We have $|y_j(P_i)|_v \ll 1$ if $v \in S_0$ and $|y_j(P_i)|_v \ll |t_v(P_i)|_v^{-n}$ if $v \in S_1$, where t_v is a local parameter at Q_v. We obtain

$$H(\mathbf{y}(P_i)) = \prod_{v \in S} \max\{1, |\mathbf{y}(P_i)|_v\} \ll \prod_{v \in S_1} |t_v(P_i)|_v^{-n}. \tag{1}$$

Now fix $v \in S_1$ and let $z_1, \dots, z_\ell$ be a basis of the filtration[2]

$$\mathcal{L} = \mathcal{L}(nD) \supset \mathcal{L}(nD - Q_v) \supset \mathcal{L}(ND - 2Q_v) \supset \dots$$

Then

$$\sum_{k=1}^{\ell} \operatorname{ord}_{Q_v} z_k \geq \sum_{k=1}^{\ell} (k - n - 1) = \frac{1}{2}\ell(\ell - 2n - 1) =: A. \tag{2}$$

Since $\ell \sim rn$ for large n, and $r \geq 3$ by the assumption, we may specify n to have $A > 0$.

Express every z_k as a linear form in $\mathbf{y}$:

$$z_k = L_{k,v}(\mathbf{y}).$$

This defines independent linear forms $L_{1,v}, \dots, L_{\ell,v}$ for $v \in S_1$. For $v \in S_0$ we simply put $L_{k,v}(\mathbf{y}) = y_k$. We obtain

$$\prod_{v \in S} \prod_{k=1}^{\ell} |L_{k,v}(\mathbf{y}(P_i))|_v \ll \prod_{v \in S'} |t_v(P_i)|_v^{\sum_{k=1}^{\ell} \operatorname{ord}_{Q_v} z_k} \leq \prod_{v \in S'} |t_v(P_i)|_v^{A},$$

where $A > 0$ is defined in (2). Combining this with (1), we obtain

$$\prod_{v \in S} \prod_{k=1}^{\ell} |L_{k,v}(\mathbf{y}(P_i))|_v \ll H(\mathbf{y}(P_i))^{-\varepsilon}$$

with $\varepsilon = A/n$.

[2] A basis of a filtration $W_0 \supseteq W_1 \supseteq W_2 \supseteq \dots$ of vector spaces is, by definition, a basis of W_0 which contains a basis of every W_i.

Now apply the Subspace Theorem. We obtain that there exist finitely many non-zero functions $u_1, \dots, u_s$ from $\mathcal{L}$ such that every P_i is a zero of one of u_j. It follows that among the points P_i only finitely many are distinct, which contradicts the original assumption about the existence of an infinite sequence of distinct S-integral points. The theorem is proved. □

2. Integral Points on Surfaces

It is widely believed that an affine (respectively, projective) variety V of general type cannot have many integral (respectively, rational) points. Of course, one cannot have here ultimate finiteness, but it is expected that integral (or rational) points are not Zariski dense on V. Faltings did the case when V is a subvariety of an abelian variety, and Vojta extended his result to subvarieties of semiabelian varieties, but very little is known for general V.

Since the argument of Corvaja and Zannier does not use Jacobians, it is very likely to extend to certain surfaces and varieties of higher dimension, the assumption *there exists at least* 3 *points at infinity* being replaced by something like *the divisor at infinity is "sufficiently reducible"*. Vojta used the Subspace Theorem to show that integral points on an irreducible affine variety of dimension d are not Zariski dense if the divisor at infinity has at least $d + \rho + 1$ components, where ρ is the rank of the Néron-Severi group.

In the article [3] Corvaja and Zannier applied their argument to integral points on surfaces. Let $\bar{X}$ be a non-singular projective surface and $X \subset \mathbb{A}^\nu$ a non-empty affine subset of $\bar{X}$. We let $C_1, \dots, C_r$ be the irreducible components of $\bar{X} \setminus X$ and we may define the "divisor at infinity" $D = C_1 + \dots + C_r$. Corvaja and Zannier, however, use the divisor

$$D = a_1 C_1 + \dots + a_r C_r$$

with some positive integers $a_1, \dots, a_r$ ("weights"). This approach is much more flexible, because the weights can be chosen in a certain "optimal" way.

Recall that in the case of curves we could apply the Subspace Theorem because for every point at infinity Q and for a sufficiently large n we found a basis $z_1, \dots, z_\ell$ of the space $\mathcal{L}(nD)$ such that $\sum_{j=1}^{\ell} \mathrm{ord}_Q(z_j) > 0$. Similarly, in the surface case, we must find, for every curve C_i and for a sufficiently large n, a basis $z_1, \dots, z_\ell$ of the space $H^0(\bar{X}, nD)$ such that $\sum_{j=1}^{\ell} \mathrm{ord}_{C_i}(z_j) > 0$.

Let $z_1, \dots, z_\ell$ be a basis of the filtration

$$H^0(\bar{X}, nD) \supseteq H^0(\bar{X}, nD - C_i) \supseteq H^0(\bar{X}, nD - 2C_i) \supseteq \dots \tag{3}$$

For this basis we have

$$\sum_{j=1}^{\ell} \mathrm{ord}_{C_i}(z_j) = -a_i n h^0(nD) + \sum_{k=0}^{\infty} h^0(nD - kC_i).$$

Thus, the basic condition to be satisfied is that the inequalities

$$\frac{\sum_{k=0}^{\infty} h^0(nD - kC_i)}{n h^0(nD)} > a_i \qquad (i = 1, \dots, r) \tag{4}$$

hold for a certain n.

Theorem 2.1 (Corvaja, Zannier)**.** *Let $\bar{X}$ be a non-singular projective surface defined over a number field K and let $X \subset \mathbb{A}^\nu$ be a non-empty affine subset of $\bar{X}$. Let $C_1, \dots, C_r$ be effective divisors*[3] *supported at $\bar{X} \setminus X$. Assume that $C_1, \dots, C_r$ intersect properly (that is, no 2 of them have a common component and no 3 of them have a common point). Further, assume that for some choice of positive integers $a_1, \dots, a_r$ the r inequalities (4) (with $D = a_1C_1 + \dots + a_rC_r$) hold for certain n. Then for any finite set $S \subset M_K$ the set $X \cap \mathbb{A}^\nu(\mathcal{O}_S)$ of S-integral points on X is not Zariski dense.*

Proof. It is quite analogous to the proof of Theorem 1.1. Let $P_1, P_2, P_3 \dots$ be sequence of distinct S-integral points; we may assume that it v-adically converges for every $v \in S$, and denote the limit by Q_v. Now we have 3 cases: either $Q_v \in X$ or Q_v belongs exactly one of the C_i (call it C_v), or it belongs to exactly two of them (call them C_v and C'_v). (By the assumption, Q_v cannot belong to three or more of C_i.) Let S_0, S_1 and S_2 be the corresponding subsets of S.

The cases $v \in S_0$ and $v \in S_1$ are treated exactly as in the proof of Theorem 1.1. For the case $v \in S_2$ one uses the following "filtration lemma", proved by induction in $\dim W$.

Lemma 2.2. *Let*

$$W = W_0 \supseteq W_1 \supseteq W_2 \supseteq \dots, \qquad W = W'_0 \supseteq W'_1 \supseteq W'_2 \supseteq \dots \tag{5}$$

be two filtrations of a finitely dimensional vector space W. Then there exists a common basis for the two filtrations (That is, there exists a basis of W containing bases for every W_i and for every W'_i.)

We leave the details of the proof to the reader. □

Imposing on our divisors C_i additional assumption (like ampleness), we can estimate from below the quantity on the left of (4) asymptotically (as $n \to \infty$), using the Riemann-Roch theorem on surfaces. After some calculation, we find that (4) holds for large n if

$$\frac{D^2}{D \cdot C_i}\left(1 + \frac{1}{6}\frac{D^2C_i^2}{(D \cdot C_i)^2}\right) > 4a_i \qquad (i = 1, \dots, r). \tag{6}$$

Levin [4], and, independently, Autissier [1] observed that a "nearly optimal" choice of the weights $a_1, \dots, a_r$ implies that 4 ample divisors at infinity would suffice. More precisely, they prove the following.

Theorem 2.3 (Levin, Autissier)**.** *Let $\bar{X}$ be a non-singular projective surface defined over a number field K and let $X \in \mathbb{A}^\nu$ be a non-empty affine subset of $\bar{X}$. Let $C_1, \dots, C_r$ be properly intersecting effective ample divisors supported at $\bar{X} \setminus X$. Assume that $r \geq 4$. Then for any finite set $S \subset M_K$ the S-integral points on X are not Zariski dense.*

[3] We do not assume the divisors $C_1, \dots, C_r$ irreducible.

Remark 2.4. In Theorem 2.3 one can relax the assumption that the divisors C_i are ample (see [4, Theorem 11.5A]), but one cannot just assume that C_i are effective and intersect properly. As an example take $\bar{X} = \mathbb{P}^1 \times \mathbb{P}^1$ and $X = \mathbb{G}_m \times \mathbb{G}_m$, where $\mathbb{G}_m$ is obtained by removing the 0-point and the ∞-point from $\mathbb{P}^1$. Then $\bar{X} \setminus X$ consists of 4 curves. The map $(x, y) \to (x, x^{-1}, y, y^{-1})$ defines an affine embedding $X \to \mathbb{A}^4$, and the set of S-integral points with respect to this embedding is $\mathcal{O}_S^\times \times \mathcal{O}_S^\times$, which is Zariski-dense in general.

To prove Theorem 2.3 we need one more elementary lemma.

Lemma 2.5. *Let $M = [\mu_{ij}]_{1 \le i,j \le r}$ be a symmetric $r \times r$-matrix with positive real entries. Consider the linear forms*

$$L_i(\mathbf{x}) = \mu_{i1}x_1 + \cdots + \mu_{ir}x_r \qquad (i = 1, \dots, r)$$

and the quadratic form $Q(\mathbf{x}) = \mathbf{x}^t M \mathbf{x}$. Then for any $\varepsilon > 0$ there exist positive integers $a_1, \dots, a_r$ such that

$$(7) \qquad (1-\varepsilon)Q(\mathbf{a}) < ra_iL_i(\mathbf{a}) \;<\; (1+\varepsilon)Q(\mathbf{a})(1-\varepsilon)Q(\mathbf{a}) < ra_iL_i(\mathbf{a}) < (1+\varepsilon)Q(\mathbf{a}) \qquad (i = 1, \dots, r),$$

where $\mathbf{a} = (a_1, \dots, a_r)$.

Proof. We follow the elegant argument of Autissier [1, Proposition 2.3]. Notice that

$$Q(\mathbf{x}) = x_1L_1(\mathbf{x}) + \cdots + x_rL_r(\mathbf{x}).$$

Hence we have to find a point $\mathbf{a}$ with positive *integral* coordinates such that the r numbers $a_iL_i(\mathbf{a})$ are *approximately* equal. We first find a point with positive *real* coordinates where these numbers are *exactly* equal.

Let Δ be the simplex

$$x_1 + \cdots + x_r = 1, \qquad 0 \le x_i \le 1 \qquad (i = 1, \dots, r).$$

By the Brower theorem, the map $\Delta \to \Delta$ defined by

$$\mathbf{x} \mapsto \left(L_1(\mathbf{x})^{-1}, \dots, L_r(\mathbf{x})^{-1}\right) \left(\sum_{i=1}^{r} L_i(\mathbf{x})^{-1}\right)^{-1}.$$

has a fixed point $\mathbf{a} \in \Delta$. For this point we have $a_1L_1(\mathbf{a}) = \ldots = a_rL_r(\mathbf{a})$. Replacing each a_i by a suitable rational approximation, we obtain positive rational numbers $a_1, \dots, a_r$ satisfying (7). Multiplying them by the common denominator, we arrive to the desired integers $a_1, \dots, a_r$. □

Proof of Theorem 2.3. First of all, remark that the term $\frac{1}{6}\frac{D^2C_i^2}{(D \cdot C_i)^2}$ is bounded from below, uniformly in $\mathbf{a}$, by a positive constant. Thus, to ensure (6), we must find positive integers $a_1, \dots, a_r$ such that for some $\varepsilon > 0$ the inequalities

$$D^2\,(1+\varepsilon) > 4a_i(D \cdot C_i) \qquad (i = 1, \dots, r)$$

hold. Applying Lemma 2.5 to the intersection matrix of $C_1, \dots, C_r$, we find $a_1, \dots, a_r$ such that

$$D^2\,(1+\varepsilon) > ra_i(D \cdot C_i) \qquad (i = 1, \dots, r).$$

Since $r \geq 4$, we are done. □

In his fundamental article [4] Levin extends Theorem 2.3 to varieties of arbitrary dimension, without assuming proper intersection. One difficulty he has to overcome is that Lemma 2.2 is no longer true for three or more filtrations.

Levin gives a thorough analysis of the argument of Corvaja and Zannier and, probably, reaches its "natural limitations". In addition, he accompanies every Diophantine result with an analogous statement about holomorphic maps, in accordance with Vojta's philosophy.

References

[1] P. Autissier, *Gé omé trie des surfaces algé briques et points entiers*, math.NT/0606184, `arxiv.org`.

[2] P. Corvaja, U. Zannier, *A Subspace Theorem approach to integral points on curves*, C. R. Acad. Sci. Paris Ser. I **334** (2002), 267–271.

[3] P. Corvaja, U. Zannier, *On integral points on surfaces*, Ann. of Math. (2) **160** (2004), 705–726.

[4] A. Levin, *Generalizations of Siegel's and Picard's Theorems*, Ann. of Math. (2), to appear; math.NT/0503699, `arxiv.org`.

On the abc conjecture in number fields

Kálmán Győry

(joint work with Kunrui Yu)

Let K be an algebraic number field of degree n with class number h and regulator R. Let M_K denote the set of places on K, and let S be a finite subset of M_K which contains all infinite places. Let $s = \mathrm{Card}(S)$, $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ the prime ideals corresponding to the finite places in S, $P = \max_i N(\mathfrak{p}_i)$, and R_S the S-regulator of K. Let $\alpha, \beta \in K^*$ with $\max(h(\alpha), h(\beta)) \leq H$ $(H \geq 1)$, where $h(.)$ denotes the absolute logarithmic height. Put $\log^* a = \max(\log a, 1)$.

Many diophantine problems can be reduced to *S-unit equations* of the form

$$\alpha u + \beta v = 1 \quad \text{in } S\text{-units } u, v \text{ of } K. \tag{1}$$

Several people, including (in chronological order) the speaker, Kotov and Trelina, Sprindzuk, Schmidt, Bombieri, Bugeaud and Győry, Bombieri and Cohen, and Bugeaud gave effective upper bounds for the solutions of (1). These led to many applications; see e.g. [2], [4], [5] and [1].

As a considerable improvement of several earlier results, we proved (cf. [8], Theorem 2) a completely explicit version of the following.

Theorem 1. *All solutions u, v of* (1) *satisfy*

$$\max(h(u), h(v)) < c_1^s (P/\log^* P) R_S H, \tag{2}$$

where c_1 is an effectively computable positive constant which depends only on n, h and R.

In terms of S, s^s was the dominating factor in the previous bounds whenever $t > \log P$. Theorem 1 provides the first upper bound not containing s^s. This improvement plays an important role in some applications; see [8], [7], [6] and Theorem 2 below. The proof of (2) depends among others on the theory of logarithmic forms.

From the explicit version of Theorem 1, we deduced the following. Let A, B, C and a, b, c, be non-zero rational integers with

$$Aa + Bb + Cc = 0$$

and with $\max(|A|, |B|, |C|) \leq H$, $|abc| > 1$, where both A, B, C and a, b, c are relatively prime.

Corollary. *We have*

$$\log \max(|a|, |b|, |c|) < c_2 (P/\log^* P) \left(\prod_{p|abc} \log p \right) \log^* H,$$

where $c_2 = 2^{10t+23} t^4$, and P and t denote the greatest prime factor and the number of distinct prime factors of abc.

For a, b, $c \in K^*$, write

$$H_K(a, b, c) = \prod_{v \in M_K} \max(|a|_v, |b|_v, |c|_v),$$

where the valuations $|.|_v$ are normalized in the usual way. Further, let

$$N_K(a, b, c) = \prod_v N(\mathfrak{p})^{\mathrm{ord}_{\mathfrak{p}} p}, \tag{3}$$

where the product is over all finite v such that $|a|_v, |b|_v, |c|_v$ are not all equal, and p is the rational prime lying below the prime ideal $\mathfrak{p}$ which corresponds to v. Denote by $P_K(a, b, c)$ the greatest factor $N(\mathfrak{p})$ in (3), and by Δ_K the absolute value of the discriminant of K. For $K = \mathbb{Q}$, the following conjecture is due to Oesterlé and Masser. The general case, in this form, was proposed by Masser [9].

abc conjecture for the number field K. *For every $\varepsilon > 0$ there exists C_ε, depending only on ε, such that*

$$H_K(a, b, c) < C_\varepsilon^n (\Delta_K N_K(a, b, c))^{1+\varepsilon}$$

for all a, b, $c \in K^*$ satisfying $a + b + c = 0$.

This conjecture has many extraordinary consequences; cf. e.g. [12], [3] and [10].

The bounds on the solutions of (1) with $\alpha = \beta = 1$ enable one to deduce bounds for $H_K(a, b, c)$. In the case $K = \mathbb{Q}$, Stewart and Yu [11] used a more direct approach to prove that if a, b, c are relatively prime positive rational integers with $a + b = c$ then

$$\log c < p' N^{c_3 \log_3 N^* / \log_2 N^*}, \tag{4}$$

where p' is the minimum of the greatest prime factors of a, b and c, respectively, $N = \prod_{p|abc} p$, $N^* = \max(N, 16)$, c_3 is an effectively computable positive absolute constant and $\log_i$ denotes the ith iterate of the log function.

From a consequence (cf. [8], Corollary 2) of the explicit version of Theorem 1, we deduced the following.

Theorem 2. *If a, b, $c \in K^*$ satisfy $a + b + c = 0$, then $\log H_K(a, b, c)$ is bounded above by*

$$c_4 \left(P/\log^* P\right) N^{(c_5 + 20n \log_3 N^*)/\log_2 N^*},$$

and, for every $\varepsilon > 0$, by

$$c_6 N^{1+\varepsilon},$$

where $P = P_K(a, b, c)$, $N = N_K(a, b, c)$, $N^* = \max(N, 16)$,

$$c_4 = 8^{3n+21} n^{6n+18} \Delta_K \left(\log^* \Delta_K\right)^{3n-1}, c_5 = 9n^3 \log^* \Delta_K$$

and $c_6 = c_6(n, \Delta_K, \varepsilon)$ is effectively computable.

For $K = \mathbb{Q}$, we obtained (4) with $c_3 = 653$ and with p' replaced by $2^{23} P/\log^* P$, where P is the greatest prime factor of abc. For number fields K of degree > 1, Theorem 2 provides the best known and the first completely explicit upper bound for $H_K(a, b, c)$.

References

[1] Y. Bugeaud, *Bornes effectives pour les solutions des équations en S-unités et des équations de Thue-Mahler*, J. Number Theory **71** (1998), 227–244.

[2] J. H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, *S-unit equations and their applications,* in *New Advances in Transcendence Theory (A. Baker ed.)*. Cambridge University Press, 1988. pp.110–174.

[3] A. Granville and T. J. Tucker, *It's as easy as abc*, Notices Amer.Math. Soc. **49** (2002), 1224–1231.

[4] K. Győry, *Some recent applications of S-unit equations*, Astérisque **209** (1992), 17–38.

[5] K. Győry, *Applications of unit equations,* in *Analytic Number Theory*, Kyoto, 1996. pp. 62–78.

[6] K. Győry, *Polynomials and binary forms with given discriminant*, Publ. Math. Debrecen **69** (2006), 473–499.

[7] K. Győry, I. Pink and Á. Pintér, *Power values of polynomials and binomial Thue-Mahler equations*, Publ. Math. Debrecen **65** (2004), 341–362.

[8] K. Győry and K. Yu, *Bounds for the solutions of S-unit equations and decomposable form equations*, Acta Arith. **123** (2006), 9–41.

[9] D. W. Masser, *On abc and discriminants*, Proc. Amer. Math. Soc. **130** (2002), 3141–3150.

[10] A. Nitaj, *The abc conjecture home page*, http://www.math.unicaen.fr/∼nitaj/abc.html, 2007.02.22.

[11] C. L. Stewart and K. Yu, *On the abc conjecture II*, Duke Math. J. **108** (2001), 169–181.

[12] P. Vojta, *Diophantine Approximation and Value Distribution Theory*, Lecture Notes in Math. **1239**. Springer-Verlag, 1987.

The reduced length of a polynomial, revisited

A. Schinzel

Length of a polynomial $P(x) = \sum_{i=0}^{d} a_i x^{d-i}$ is $L(P) = \sum_{i=0}^{d} |a_i|$. For $P \in \mathbb{R}[x]$ A. Dubickas [2] introduced the reduced length

$$l(P) = \inf_{Q \in \mathbb{R}[x],\, Q\text{-monic}} L(PQ)$$

and noticed that if $P = P_0 P_1$, where all zeros of P_1 are inside the unit circle C then

$$l(P) = l(P_0).$$

Thus the problem remains to compute $l(P)$, if all zeros of P are outside C or on C. In [2] I have shown how to compute $l(P)$ if all zeros are outside C, or all zeros are an C, or there is just one zero, possibly multiple, on C and all other zeros are real of the same sign. This suffices to compute $l(P)$ for all quadratic polynomials, but for cubic polynomials there remain two cases.

(1) P has just one zero on C, but the other zeros are either complex or real of opposite sign.
(2) P has just two zeros on C.

The first case can be settled completely.

Theorem 1. *If $P(x) = \prod_{i=1}^{3}(x - \alpha_i)$, where $|\alpha_1| \geq |\alpha_2| > |\alpha_3| = 1$, $\alpha_1 \neq \alpha_2$, then $l(P)$ can be effectively computed.*

The idea of the proof is to indicate for every n in $\mathbb{N}$ a finite set S_n of monic polynomials divisible by P such that $0 \geq l(P) - \min_{Q \in S_n} L(Q) > -\frac{1}{n}$.

Corollary. *Let $P^*(x) = x^{\deg P} P(x^{-1})$. Then, for every cubic $P \in \mathbb{R}[x]$, $\hat{l}(P) = \min\{l(P), l(P^*)\}$ can be effectively computed.*

The corollary is of interest, since $\hat{l}(P)$, rather than $l(P)$ occurs in applications given in [1].

The second case is really difficult and I cannot compute $l(P)$, already for $P = 2x^3 + 3x^2 + 4$. The computation can be made, however, if the zeros of P on C are roots of unity and as an example I give

Theorem 2. *Let $P(x) = (x - \alpha)(x^2 - \varepsilon)$, where $|\alpha| > 1$, $\varepsilon = \pm 1$. Then*

$$l(P) = 2\big(|\alpha| + 1 - |\alpha|^{-1}\big).$$

In connection with Theorem 2 I propose the following

Problem. *Is the inequality*

$$l\left(\left(x^2 + tx + 1\right) P(x)\right) \geq 2M(P)$$

where $M(P)$, is the Mahler measure, true for all $t \in [-2, 2]$ and all $P \in \mathbb{R}[x]$?

Theorems 1 and 2 are proved in [3].

References

[1] A. Dubickas, *Arithmetical properties of powers of algebraic numbers*, Bull. London Math. Soc., 38 (2006), 70–80.

[2] A. Schinzel, *On the reduced length of a polynomial with real coefficients*, in: A. Schinzel, Selecta, vol. 1, 658–691.

[3] A. Schinzel, *On the reduced length of a polynomial with real coefficients II*, Funct. Approximatio Comment. Math. (to appear).

Cubic Thue equations with many solutions

Cameron Stewart

Let $F(x, y)$ be a cubic binary form with integer coefficients and non-zero discriminant. Let m be a positive integer and let $N_F(m)$ be the number of solutions of the Thue equation

$$F(x, y) = m,$$

in integers x and y. Following an approach introduced by Chowla in 1933, Mahler proved, in 1935, that there is a positive number c_1, which depends on F, such that

$$N_F(m) > c_1(\log m)^{1/4}, \tag{1}$$

for infinitely many positive integers m. This was refined by Silverman in 1983. He proved that the exponent $1/4$ in (1) may be replaced by $1/3$. In our talk we indicated how we are now able to replace the exponent of $1/4$ in Mahler's result by the exponent $1/2$.

Small value estimates for the multiplicative group

Damien Roy

Define the *height* $H(P)$ of a polynomial $P \in \mathbb{Z}[T]$ to be the maximum of the absolute values of its coefficients. In an attemp to extend to the multiplicative group $\mathbb{G}_{\mathrm{m}}$ the results of [3], we present the following transcendence criterion dealing with a sequence of integer polynomials taking small values on complex numbers from a fixed geometric progression.

Theorem. *Let $\xi \in \mathbb{C}$ and let $\beta, \sigma, \nu \in \mathbb{R}$ such that*

$$0 \le \sigma \le \frac{11}{7}, \quad \beta \ge 1 + \sigma, \quad \nu > 1 + \beta - \frac{5}{11}\sigma. \tag{1}$$

Suppose that, for each sufficiently large positive integer n, there exists a non-zero polynomial $P_n \in \mathbb{Z}[T]$ satisfying

$$\deg(P_n) \le n, \ H(P_n) \le \exp(n^\beta), \ \max\{|P_n(\xi^i)| \, ; \, 1 \le i \le n^\sigma\} < \exp(-n^\nu). \tag{2}$$

Then ξ is algebraic over $\mathbb{Q}$.

In the case where $\sigma = 0$, this result reduces to a well-known version of Gel'fond's transcendence criterion due to D. W. Brownawell [1] and M. Waldschmidt [4]:

Gel'fond's Criterion (Brownawell, Waldschmidt)**.** *Let $\xi \in \mathbb{C}$ and let $\beta, \nu \in \mathbb{R}$ with $\beta \geq 1$ and $\nu > 1 + \beta$. Suppose that for each sufficiently large positive integer n, there exists a non-zero polynomial $P_n \in \mathbb{Z}[T]$ satisfying* $\deg(P_n) \leq n$, $H(P_n) \leq \exp(n^\beta)$ *and* $|P_n(\xi)| < \exp(-n^\nu)$. *Then ξ is algebraic over $\mathbb{Q}$.*

The condition on ν in the theorem is weaker than that required by Gel'fond's criterion, with a saving of $(5/11)\sigma$. On the other hand, a simple application of Dirichlet box principle shows that, given $\xi \in \mathbb{C}$ and $\beta, \sigma, \nu \in \mathbb{R}$ with $0 \leq \sigma < 1$, $\beta > 2\sigma$ and $\nu < 1 + \beta - \sigma$, there exists for each sufficiently large index n a non-zero polynomial $P_n \in \mathbb{Z}[T]$ satisfying (2). So it is possible that the last condition in (1) could be improved to $\nu > 1 + \beta - \sigma$, which would then be best possible.

Sketch of proof. Assume for simplicity that $|\xi| \neq 1$. We present a sketch of proof of the theorem with the last condition in (1) replaced by the stronger condition $\nu > 1 + \beta - (1/3)\sigma$. For the first four steps of the argument, we fix an arbitrary large integer n and write $P = P_n$ for simplicity.

1. Reduction: Without loss of generality, we may assume that $P(0) \neq 0$ and that no root of P is a root of unity.

2. Let $\mu \in \mathbb{R}$ with $0 < \mu < \sigma$, and let A be the set of all prime numbers p with $(1/2)n^\mu \leq p \leq n^\mu$. Then the gcd $Q \in \mathbb{Z}[T]$ of the polynomials $P(T^a)$ with $a \in A$ satisfies

$$\deg(Q) \ll \frac{n}{|A|} \asymp n^{1-\mu} \log(n) \quad \text{and} \quad \log H(Q) \ll \frac{n^\beta}{\sum_{a \in A} a} \asymp n^{\beta - 2\mu} \log(n),$$

with implied constants depending only on μ. These estimates are optimal up to the value of the constants and require simply that $\beta \geq 1 + \mu$ (provided that P does not vanish at 0 nor at any root of unity). They are proved by combinatorial arguments.

3. Let D be a subset of $\{1, 2, \ldots, [n^{\sigma-\mu}]\}$. Assume that $\beta \geq 1+\sigma$, $\mu < \sigma < 1+2\mu$ and $|D|n^\nu > 10n^{1+\beta+\mu}$. Then, if n is sufficiently large, we have

$$\prod_{i \in D} |Q(\xi^i)| \leq \exp\Big(-\frac{1}{2}|D|n^\nu \Big).$$

The proof of this is similar to that of Lemma 13 of [2]. It proceeds by estimating from above the height of the U-resultant of the polynomials $P(T^a)/Q(T)$ $(a \in A)$ upon noting that all of these take small values at the points ξ^i with $i \in D$.

4. By Part 3 above, there exists an element i of D with $|Q(\xi^i)| \leq \exp(-(1/2)n^\nu)$. Put $R_n(T) = Q(T^i)$. Since $i \leq n^{\sigma-\mu}$, the estimates of Part 2 imply that the polynomial $R_n \in \mathbb{Z}[T]$ satisfies

$$\deg(R_n) \ll n^{1+\sigma-2\mu} \log(n) \quad \text{and} \quad \log H(R_n) \ll n^{\beta-2\mu} \log(n).$$

5. Applying Gel'fond's criterion to the sequence of polynomials R_n, we deduce that ξ is algebraic over $\mathbb{Q}$ if

$$\nu > (1 + \sigma - 2\mu) + (\beta - 2\mu).$$

If we choose $\mu = \sigma/3$ and take D to be the set of all integers in the interval $[1, n^{\sigma-\mu}]$, then all the above conditions are satisfied provided that $\sigma < 3$, $\beta \geq 1 + \sigma$ and $\nu > 1 + \beta - \sigma/3$. □

References

[1] W. D. Brownawell, *Sequences of Diophantine approximations*, J. Number Theory **6** (1974), 11-21.

[2] M. Laurent and D. Roy, *Criteria of algebraic independence with multiplicities and interpolation determinants*, Trans. Amer. Math. Soc. **351** (1999), 1845–1870.

[3] D. Roy, *Small value estimates for the additive group*, preprint, 32 pages.

[4] M. Waldschmidt, *Solution du huitième problème de Schneider*, J. Number Theory **5** (1973), 191–202.

On additive equations in positive characteristic

David Masser

Let K be a field and let G be a multiplicative subgroup of the group of non-zero elements of K. For $n \geq 2$ and a variety V in $\mathbf{P}_n$ write $V(G)$ for the set of points on V with projective coordinates in G. With Harm Derksen we gave a completely effective description of $V(G)$ when K has positive characteristic, G is finitely generated, and V is linear.

Write $\sqrt{G} = \sqrt[K]{G}$ for the radical of G (inside K) consisting of all x in K for which there is k in $\mathbf{N}$ with x^k in G. Call a linear variety V transversal if every coordinate $X_0, \ldots, X_n$ occurs (with non-zero coefficient) in the defining equations. Call it G-isotrivial if there are $g_0, \ldots, g_n$ in G such that the isomorphism $\psi(X_0, \ldots, X_n) = (g_0 X_0, \ldots, g_n X_n)$ sends V to a variety defined over a finite field.

Theorem. *Suppose that K has positive characteristic and that V is defined over K and transversal. Suppose further that $\sqrt{G}$ is finitely generated. Then there is an effectively computable finite collection $\mathcal{W}$ of proper $\sqrt{G}$-isotrivial linear subvarieties W of V, also defined over K, such that*
(a) if V is not $\sqrt{G}$-isotrivial, then

$$V(G) = \bigcup_{W \in \mathcal{W}} W(G),$$

(b) if V is $\sqrt{G}$-isotrivial and $\psi(V)$ is defined over $\mathbf{F}_q$, then

$$V(G) = \psi^{-1}\left(\bigcup_{W \in \mathcal{W}} \bigcup_{e=0}^{\infty} (\psi(W)(G))^{q^e} \right).$$

Thus we can always descend to lower dimension. After at most $\dim V \leq n - 1$ such descents we end up with an effective description of the solution set in terms of a finite subset and a finite set of isomorphisms, together with at most $n - 1$ Frobenius actions; the latter generally do not commute with each other.

The effectivity can be made explicit in terms of a suitable height function $h(V)$ and a related regulator function $R(G)$. In the special case $G = \sqrt{G}$ one even gets a polynomial dependence on these functions. However in general one should allow an exponential dependence on $R(G)$, and there are examples to show that this cannot be avoided.

The result can be used to solve diophantine equations in positive characteristic involving several recurrence sequences, say $u_1, \dots, u_m$ taking values in K on $\mathbf{N}$; for example one can decide whether or not there exist $r_1, \dots, r_m$ in $\mathbf{N}$ such that

$$u_1(r_1) + \cdots + u_m(r_m) = 0.$$

This may be compared with a conjecture of Cerlienco, Mignotte and Piras [CMP] (p.104) that such problems can be undecidable in zero characteristic.

The result, apart from the effectivity, is a natural analogue of the classical result of van der Poorten and Schlickewei in zero characteristic for $\dim V = n - 1$.

The results in both characteristics, despite the apparent lack of effectivity in one of them, nevertheless enable one to find effectively the smallest order of non-mixing of a given algebraic $\mathbf{Z}^d$-action on a compact abelian group.

The impetus to consider these problems came from two sources: first Masser's paper [M], which uses Wronskians as in situations of *abc* type to reduce to p-th powers, and second Derksen's recent paper [D], where formally similar reductions, but without derivatives, are carried out in the language of automata theory.

There is an independent literature in the more general context of Mordell-Lang problems on semiabelian varieties (Abramovich-Voloch 1992, Hrushovsky 1996, Voloch 1998, Moosa-Scanlon 2002, 2004, Ghioca to appear). When specialized, some of the results seem related to ours, but the authors do not discuss effectivity, apart from Voloch. His paper proves (a) above when $n = 2$ and gives a good explicit upper bound for the number of W. He also uses derivatives, but the other authors use among other things Hilbert schemes, model theory and ultrafilters.

References

[CMP] L. Cerlienco, M. Mignotte, F. Piras, *Suites récurrentes linéaires: propriétés algébriques et arithmétiques,* L'Enseignement Mathématique **33** (1987), 67-108.

[D] H. Derksen, *A Skolem-Mahler-Lech theorem in positive characteristic and finite automata,* Inventiones Math. **168** (2007), 175-224.

[M] D. W. Masser, *Mixing and linear equations over groups in positive characteristic,* Israel J. Math. **142** (2004), 189-204.

Relations on a power of an elliptic curve

Philipp Habegger

Let A be a semi-abelian variety defined over $\mathbf{C}$ and let $X \subset A$ be an irreducible closed subvariety. The intersection of X with the division closure of a finitely generated subgroup of A has been studied by Faltings, Hindry, Laurent, McQuillan, Raynaud, Vojta and others. In 1995 this work culminated in the proof of the Mordell-Lang conjecture.

More recently, interest has arose in analyzing the intersection of X with $A^{[r]}$, the union of all algebraic subgroups of A with codimension at least r. Motivated by a specialization of Silverman, early results were obtained by Bombieri, Masser, and Zannier [1] in the algebraic torus $\mathbf{G}_m^n$. More precisely, they showed that if C is an algebraic curve defined over $\overline{\mathbf{Q}}$ not contained in the translate of a proper algebraic subgroup, then the points in $C \cap (\mathbf{G}_m^n)^{[1]}$ have uniformly bounded Weil height. Using this height upper bound and Lehmer-type lower bounds for heights, they also showed that $C \cap (\mathbf{G}_m^n)^{[2]}$ is finite.

An irreducible subvariety Y of X is called anomalous if $\dim Y \geq 1$ and if Y is contained in the translate of a proper algebraic subgroup K of A such that $\dim Y \geq \dim X + \dim K - \dim A + 1$. Such a Y is contained in an improper component of the intersection $X \cap K$. We define X^{oa} to be X deprived of all its anomalous subvarieties.

When the semi-abelian variety is $\mathbf{G}_m^n$, this definition appeared in a preprint [3] of Bombieri, Masser, and Zannier. They proved that X^{oa} is Zariski open in X. If X is defined over $\overline{\mathbf{Q}}$ they stated the Bounded Height Conjecture: $X^{\mathrm{oa}}(\overline{\mathbf{Q}}) \cap (\mathbf{G}_m^n)^{[\dim X]}$ has uniformly bounded Weil height. The lower bound $\dim X$ imposed on the codimension of the algebraic subgroups involved is best-possible.

If A is defined over $\overline{\mathbf{Q}}$ and given a suitable height function on $A(\overline{\mathbf{Q}})$ it is straightforward to formulate the Bounded Height Conjecture for subvarieties of an arbitrary semi-abelian variety.

We consider the case $A = E^g$ where E is an elliptic curve defined over $\overline{\mathbf{Q}}$. Let $\hat{h}$ be the Néron-Tate height associated to a symmetric and ample line bundle on E^g. The purpose of this talk is to present a proof of the Bounded Height Conjecture in E^g:

Theorem 1. *Let $X \subset E^g$ be an irreducible closed subvariety defined over $\overline{\mathbf{Q}}$, then $X^{\mathrm{oa}} \subset X$ is Zariski open, furthermore the Néron-Tate height $\hat{h}$ is bounded on $X^{\mathrm{oa}}(\overline{\mathbf{Q}}) \cap (E^g)^{[\dim X]}$.*

If X is generic in a certain sense which will not be specified here, then X^{oa} will be non-empty, hence Zariski dense in X.

As in Bombieri, Masser, and Zannier's original article on curves it is possible to deduce a finiteness result when the algebraic subgroups involved have codimension at least $1 + \dim X$ as soon as a sufficiently strong Lehmer-type height lower bound is known. Indeed, recent work of Ratazzi [4] on such bounds for abelian varieties with complex multiplication suffices to prove:

Theorem 2. *Let X be as in Theorem 1, then $X^{\mathrm{oa}}(\overline{\mathbf{Q}}) \cap (E^g)^{[1+\dim X]}$ is finite.*

Bombieri, Masser, and Zannier noticed [1] that X^{oa} is most likely not the correct set for a finiteness statement as in Theorem 2. One generally believes that finiteness holds with X^{oa} replaced by a possibly larger set X^{ta}. The definition of X^{ta} is verbatim to X^{oa} with the exception that K is required to be the translate of an algebraic subgroups by a torsion point. Some finiteness results in abelian varieties have been obtained by Ratazzi, Rémond, and Viada.

To prove Theorem 1 one is lead to the study of the following function involving the degree of a morphism:

$$f_X(\varphi) = \deg(\varphi|_X)$$

here $r = \dim X$ and $\varphi : E^g \to E^r$ is a homomorphism of abelian varieties with $\varphi|_X$ its restriction to X. For simplicity let us assume that E does not have complex multiplication. Then φ may be identified with an $r \times g$ matrix in integer coefficients. By the Theorem of the Cube f_X is polynomial with rational coefficients in the entries of φ; more precisely it is homogeneous of degree 2 in each line of φ. This polynomial is invariant under left-multiplication of φ by an element of $\mathrm{SL}_r(\mathbf{C})$. Therefore we may write f_X as β_X, a quadratic form with rational coefficients in the $N = \binom{g}{r}$ Plücker coordinates of the matrix φ. Considering the Plücker embedding of the Grassmannian $G(r,g) \hookrightarrow \mathbf{P}^{N-1}$ one can show that

$$X^{\mathrm{oa}} \neq \emptyset \text{ if and only if } \beta_X \text{ is (strictly) positive on } G(r,g)(\mathbf{Q}).$$

We note that although the value of β_X at a point of $\mathbf{P}^{N-1}(\mathbf{R})$ is not well-defined, its sign is since β_X is a quadratic form. In the crucial step of the proof of Theorem 1 we use analytic geometry and a Theorem of Ax [2] to show that

(1) β_X is positive on $G(r,g)(\mathbf{Q})$ if and only if β_X is positive on $G(r,g)(\mathbf{R})$.

We have therefore established a strong Hasse principle for β_X: this quadratic form vanishes on $G(r,g)(\mathbf{R})$ if and only if it vanishes on $G(r,g)(\mathbf{Q})$. Assuming β_X does not vanish on $G(r,g)(\mathbf{R})$, we can apply a compactness argument to deduce a lower bound for the degree

$$\deg(\varphi|_X) \geq c(X) \det(\varphi\varphi^{\mathrm{T}}) \tag{2}$$

where $c(X) > 0$ is independent of φ. This uniformity in φ is essential for the proof of Theorem 1. The degree is essentially the self-intersection number of a certain line bundle related to φ. Using the theory of heights associated to line bundles and a Theorem of Siu, inequality (2) translates into a uniform inequality of heights. This height inequality is the main ingredient in the proof of Theorem 1.

In the special case where X is a curve or hypersurface, that is if $r = 1$ or $r = g - 1$, one has $G(r,g) = \mathbf{P}^{g-1}$. By a classical result any quadratic form with rational coefficients with is positive on $\mathbf{Q}^N \backslash \{0\}$ is also positive on $\mathbf{R}^N \backslash \{0\}$. In other words: if $r \in \{1, g-1\}$ then a quadratic form β in rational coefficients is positive on $G(r,g)(\mathbf{Q})$ if and only it is positive on $G(r,g)(\mathbf{R})$. Hence in this case (1) follows without using analytic geometric or Ax's Theorem. But for general r and g we need these tools. Indeed let us consider the example $r = 2$ and $g = 4$.

Then $G(2,4) \subset \mathbf{P}^5$ has dimension 4. If $\Delta_0, \ldots, \Delta_5$ denote projective coordinates on $\mathbf{P}^5$, then $G(2,4)$ is defined by one Plücker relation $\Delta_0\Delta_5 - \Delta_1\Delta_4 + \Delta_2\Delta_3 = 0$. The quadratic form $\beta = (\Delta_0 - 2\Delta_5)^2 + (\Delta_1 - \Delta_4)^2 + \Delta_2^2 + \Delta_3^2$ is positive on $G(2,4)(\mathbf{Q})$ since $\sqrt{2}$ is irrational. On the other hand $\beta(2, \sqrt{2}, 0, 0, \sqrt{2}, 1) = 0$, hence β vanishes on $G(2,4)(\mathbf{R})$. In particular this β cannot equal β_X coming from an algebraic surface X in E^4.

References

[1] E. Bombieri, D. Masser, and U. Zannier, *Intersecting a curve with algebraic subgroups of multiplicative groups*, Int. Math. Res. Not. **20** (1999), 1119-1140.

[2] James Ax, *Some topics in differential algebraic geometry I: Analytic subgroups of algebraic groups*, Amer. J. Math. **94** (1972), 1195-1204.

[3] E. Bombieri, D. Masser, and U. Zannier, *Anomalous subvarieties - structure theorems and applications*, Preprint (2006).

[4] Nicolas Ratazzi, *Intersection de courbes et de sous-groupes, et problèmes de minoration de hauteur dans les variétés abéliennes C.M.*, Preprint (2007).

A lower bound for the essential minimum in a product of elliptic curves

Aurélien Galateau

1. Introduction

Let C be an algebraic curve with genus $g \geq 2$ defined on $\bar{\mathbb{Q}}$ and embedded in its jacobian $J(C)$. Thus, there is a canonical height $\hat{h}$ for points of $J(C)$. Extending the Manin-Mumford conjecture (concerning torsion points, that is: points with height zero), one can ask if there are a lot of points with small height lying in the curve. In 1981, Bogomolov conjectured the following:

Conjecture 1. *There exists $\epsilon > 0$ such that $\{x \in C(\bar{\mathbb{Q}}), \hat{h}(x) \leq \epsilon\}$ is finite.*

Let now V be an algebraic subvariety of S a semi-abelian variety. In higher dimension, finiteness is replaced by non Zariski density; semi abelian subvarieties and their translates have a lot of small points (at least their torsion points). Define the essential minimum :

$$\hat{\mu}_{ess}(V) = \inf\{\theta > 0, \overline{V(\theta)} = V(\overline{\mathbb{Q}})\},$$
$$\text{where } V(\theta) = \{x \in V(\bar{\mathbb{Q}}), \hat{h}(x) \leq \theta\}.$$

The generalisation of the Bogomolov conjecture then says:

Conjecture 2. *The essential minimum of V is zero if and only if $V = x + B$ with x torsion and B a semi-abelian subvariety of S.*

The first conjecture was proved by Ullmo in 1998 and the second by Zhang for abelian varieties and tori, by David and Philippon for semi abelian varieties.

2. Explicit version

Once qualitative conjectures are solved, one can ask for an explicit version, that is: say more about the essential minimum provided it is non zero. Thanks to the inequality on successive minima proved by Zhang, this would also give information about the height of V. The invariants concerned for bounding the essential minimum will be the dimension and the degree of V, a term measuring the height of S and the degree of a definition field.

In the case of tori, Amoroso and David gave a lower bound optimal up to logarithmic factors in the degree of V and further, their bound was thoroughly explicit. The theorem of David and Philippon was also explicit but not optimal yet in the degree. The aim of my work was to get the same results in the abelian context as those already known for tori. In this direction, one obtains the following:

Theorem 3. *Let V be a proper and irreducible subvariety of $A = E_1 \times \ldots \times E_g$ a product of elliptic curves ($g \geq 2$), with codimension k. If V is not contained in any translate of a proper abelian subvariety of A, the following holds:*

$$\hat{\mu}_{ess}(V) \geq \frac{C(A)}{\omega(V)} \times (\log(3\omega(V)))^{-\lambda(k,g)},$$

where $C(A) > 0$ is a constant depending only on A and $\lambda(k, g) = (9g(3k)^{(k+1)})^k$.

3. Diophantine approximation

The proof of the last theorem is classical diophantine approximation. Suppose V is a subvariety with essential minimum unexpectedly large. Using an absolute Siegel lemma, one proves that there is an auxiliary function which vanishes on the subvariety with high order. The extrapolation is made using torsion points. Therefore, one proves that the function is zero on a lot of translates of V by 'good' torsion points, but the new order is weaker. For technical reasons, one has to iterate this step. One then shows that the union of varieties on which the auxiliary function vanishes is large by working on the stabilisator and using combinatorics. A zero lemma finally compares the degree of the union to the function's degree and gives a contradiction.

The extrapolation step is based on a p-adic inequality that is the analogue of the following easy fact:

Lemma 4. *For all ξ a p^{th}-root of the unity and all v/p a place of $\mathbb{Q}[\xi]$:*

$$|\xi - 1|_v \leq p^{-1/p}.$$

Using the theory of formal groups, one gets the same estimate in the elliptic setting provided that the prime p is an ordinary prime (for supersingular primes, one gets: p^{-1/p^2}). Since such primes are in positive density (1/2 for CM curves and 1 for non CM), it is possible to find a set of primes with positive density being simultaneously ordinary for all the elliptic curves in A.

That kind of argument should be refined for abelian varieties, since no result of density is known for ordinary primes. Nevertheless, weaker p-adic properties could be balanced by a larger number of torsion points reducing on zero, for which the p-adic property holds.

A complete metric space arising from the logarithmic Weil height

Jeffrey D. Vaaler
(joint work with Daniel Allcock)

Let $h : \overline{\mathbb{Q}}^\times \to [0, \infty)$ denote the absolute logarithmic Weil height. We recall that this is defined by

$$h(\alpha) = \sum_v \log^+ |\alpha|_v,$$

where the sum is over all places v of a number field k that contains α and $|\ |_v$ is a certain normalized absolute value from the place v. It is obvious from the definition that $h(\alpha) = h(\zeta\alpha)$ for all points α in $\overline{\mathbb{Q}}^\times$ and all ζ in the torsion subgroup $\mathrm{Tor}\big(\overline{\mathbb{Q}}^\times\big)$. Therefore the height h is well defined as a map on the quotient group

$$h : G \to [0, \infty) \quad \text{where} \quad G = \overline{\mathbb{Q}}^\times / \mathrm{Tor}\big(\overline{\mathbb{Q}}^\times\big). \tag{1}$$

If α and β are points in the group G then (1) satisfies

(i) $h(\alpha) = 0$ if and only if $\alpha = 1$ in G,
(ii) $h(\alpha^{-1}) = h(\alpha)$,
(iii) $h(\alpha\beta) \le h(\alpha) + h(\beta)$.

It follows that the map $(\alpha, \beta) \to h(\alpha\beta^{-1})$ defines a metric on the group G and so induces a metric topology in G. We are interested in the problem of describing the completion $\widehat{G}$ of this group.

As a first approach to this problem we note that the group G is also a vector space over the field $\mathbb{Q}$ of rational numbers. To see this observe that if r/s is a rational number with r and s relatively prime integers and s positive, if α is a point in $\overline{\mathbb{Q}}^\times$, then all roots in $\overline{\mathbb{Q}}^\times$ of the polynomial equations

$$X^s - (\zeta\alpha)^r = 0, \quad \text{where} \quad \zeta \in \mathrm{Tor}\big(\overline{\mathbb{Q}}^\times\big),$$

are representatives of the same coset in G. We regard this coset as $\alpha^{r/s}$ and then

$$(r/s, \alpha) \to \alpha^{r/s}$$

is easily seen to define a scalar product on the abelian group G. We find that

$$h\big(\alpha^{r/s}\big) = \big|r/s\big|_\infty h(\alpha).$$

This shows that $\alpha \to h(\alpha)$ defines a norm on the vector space G with repsect to the usual archimedean absolute value $|\ |_\infty$ on the field of scalars $\mathbb{Q}$. From this it follows that the completion $\widehat{G}$ is a Banach space over the field $\mathbb{R}$ or real numbers. It remains now to give a more precise description of this Banach space.

Let $\mathcal{L}$ be the set of all intermediate fields k such that $\mathbb{Q} \subseteq k \subseteq \overline{\mathbb{Q}}$ and such that k is a finite extension of $\mathbb{Q}$. Then $\mathcal{L}$ is partially ordered by inclusion and is a directed set. For each field k in $\mathcal{L}$ and place p of $\mathbb{Q}$, let $V(k,p)$ denote the set of places v of k such that $v|p$. (Here p may be archimedean or non-archimedean.) Let Ω be the set of all places of $\overline{\mathbb{Q}}$. Then Ω can be realized as the inverse limit of the finite sets $V(k,p)$ and in this way Ω is given a totally disconnected, locally compact, Hausdorff topology. The absolute Galois group $\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on points of Ω and this can be used to prove the existence of a certain nontrivial, invariant measure ν on the Borel subsets of Ω. Thus we may consider the real Banach space $L^1(\Omega,\nu)$ and the codimension 1 subspace $\mathcal{X}$ defined by

$$\mathcal{X} = \Big\{ F \in L^1(\Omega,\nu) : \int_\Omega F(\omega)\ \mathrm{d}\nu(\omega) = 0 \Big\}.$$

If ω is an element of Ω, write $\| \ \|_\omega$ for an absolute value from the place ω that extends the usual absolute value $\mathbb{Q}$. Then for each point α in the group G let $f_\alpha : \Omega \to \mathbb{R}$ be defined by

$$f_\alpha(\omega) = \log \|\alpha\|_\omega.$$

We show that f_α is a continuous function on Ω with compact support and the set of all such functions is dense in the subspace $\mathcal{X}$. Moreover, the map

$$\alpha \to f_\alpha$$

is an isometric isomorphism from G onto a dense subset of $\mathcal{X}$. More precisesly, we find that

$$h(\alpha) = \tfrac{1}{2} \int_\Omega |f_\alpha(\omega)|\ \mathrm{d}\nu(\omega).$$

It follows that we may identify G with this dense subset and conclude that $\widehat{G}$ is isometrically isomorphic to the real Banach space $\mathcal{X}$.

Cyclotomic norm equations and short vectors in lattices

Preda Mihailescu

Let p, q be two odd primes, which may also be equal. The cyclotomic norm equations under investigation are special cases of the general form

$$\begin{aligned} \frac{X^p + Y^p}{X+Y} &= p^e \cdot Z^q, \quad \text{with } X,Y,Z \in \mathbb{Z} \text{ with } (X,Y,Z) = 1 \text{ and} \\ e &= \begin{cases} 0 & \text{if } (p,Z) = 1 \\ 1 & \text{otherwise .} \end{cases} \end{aligned} \tag{1}$$

The literature below is a small selection of papers which bring important contributions to the general or some special case of (1) and have detailed historical indications; the results in this abstract are proved in [Mi1, Mi2, Mi3].

The specialization of (1) may be done by fixing one of the variables and/or adding the equation $X+Y=p^{-e}T^q$, which leads together with (1) to the Fermat - Catalan equation

$$X^p+Y^p=Z^q. \tag{2}$$

The methods used are of cyclotomic nature and they combine class field conditions with some new approximation techniques, which are closely related to the problem of short vectors in affine lattices.

In the case of three independent variables, one obtains *lower bounds* for the solutions. The following result illustrates the more general statements on (2) which we obtain:

Theorem 1. *Let $p,q>3$ be primes such that (2) has a solution and suppose that $-1\in<p \mod q>$, $\max\{p,\frac{p(p-20)}{16}\}>q$ and $q\not| h_{pq}^-$, the relative class number of the $pq-$*th *cyclotomic field. Then either*

$$a^{q-1}\equiv 1 \mod q^2 \quad \textit{for some} \quad a\in\{2,p,2^{p-1}\cdot p^p\}, \tag{3}$$

or

A. *$p\not| z$ and $q^2|xy$ if $q\not\equiv 1 \mod p$ and $q^3|xy$, if $q\equiv 1 \mod p$.*

B. *If $q\not\equiv 1 \mod p$, then*

$$\min(|x|,|y|)>c_1(q)\left(\frac{q^{p-1}}{p}\right)^{q-2}, \quad \textit{if} \quad q\not\equiv 1 \mod p, \tag{4}$$

and

$$\min(|x|,|y|)>c_1(q)\left(\frac{q^{2(p-1)}}{p}\right)^{q-2}, \tag{5}$$

otherwise. Here $c_1(q)$ is am effectively computable, strictly increasing function with $c_1(5)>1/2$.

This yields on the one hand some conditions on p,q for which the *special* Fermat - Catalan equation with fixed $Y=C$ has no solutions. An other interesting specialization is the equation $X^p+Y^q=Z^{pq}$ which is equivalent to the *Catalan equation in the rationals*. The result is then:

Theorem 2. *Let $p,q>3$ be distinct primes for which the following conditions are true:*

1. $-1\in<p \mod q>$ *and* $-1\in<q \mod p>$,
2. $\left(pq,h_{pq}^-\right)=1$,
3. $2^{p-1}\not\equiv 1 \mod p^2$ *and* $2^{q-1}\not\equiv 1 \mod q^2$,
4. $\left(2^{p-1}p^p\right)^{q-1}\not\equiv 1 \mod q^2$ *and* $\left(2^{q-1}q^q\right)^{p-1}\not\equiv 1 \mod p^2$,
5. $p^{q-1}\not\equiv 1 \mod q^2$ *and* $q^{p-1}\not\equiv 1 \mod p^2$,
6. $\max\{p,\frac{p(p-20)}{16}\}>q$ *and* $\max\{q,\frac{q(q-20)}{16}\}>p$.

Then the equation $X^p+Y^q=1$ has no rational solutions.

By fixing $Y = -1$ in (1), one obtains the equation of Nagell and Ljunggren. In this case, the approximation methods yield effective upper bounds for possible solutions of the equation. In this talk we treated the *diagonal* case with $p = q$ in more detail. This is:

$$\frac{x^p - 1}{x - 1} = p^e \cdot y^p \quad \text{with} \quad x, y \in \mathbb{Z}, \quad e \in \{0, 1\}, \tag{6}$$

and p an odd prime. The only known non - trivial solution is

$$\frac{18^3 - 1}{18 - 1} = 7^3, \tag{7}$$

and it is conjectured to be also the only such solution. The upper bounds for solutions of (6), are the following:

Theorem 3. *Suppose that x, y are integers verifying (6) and $p \geq 17$. Then there is a $B \in \mathbb{R}_+$ such that $|x| < B$. The values of B in the various cases of the equation are the following:*

$$B = \begin{cases} 4 \cdot \left(\frac{p-3}{2}\right)^{\frac{p+2}{2}} & \text{if } (x \bmod p) \notin \{-1, 0, 1\} \\ (4p)^{\frac{p-1}{2}} & \text{if } x \equiv 0 \bmod p, \\ 4 \cdot (p-2)^p & \text{otherwise.} \end{cases} \tag{8}$$

Using better lattice methods, the bounds can currently be improved to $O(p^c)$ for some positive constant $c < 20$. Similar results are obtained for the case $p \neq q$.

The general idea of proof is the following: a solution $(x, y; p)$ of (6) leads in the $p-$th cyclotomic field $\mathbb{Q}(\zeta)$ – with ζ an $p-$th root of unity – to the existence of an

$$\alpha = \frac{x - \zeta}{(1 - \zeta)^e} \in \mathbb{Z}[\zeta] \quad \text{with} \quad \mathbf{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\alpha) = y^p.$$

There is an ideal $\mathcal{A} = (\alpha, y) \subset \mathbb{Z}[\zeta]$ with $\mathfrak{A}^p = (\alpha)$. Let $G =$ Gal $(\mathbb{Q}(\zeta)/\mathbb{Q})$ and $I \subset \mathbb{Z}[G]$ be the Stickelberger ideal. Using annihilation by various elements $\Theta \in I$, one obtains $\beta[\Theta] \in \mathbb{Z}[\zeta]$ verifying:

$$\beta^p[\Theta] \quad = \quad \alpha^\theta. \tag{9}$$

With the series expansion of the $p-$th root (9) leads to approximations of $\beta[\Theta]$ up to $p-$th root of unity. More precisely, there are positive integers $k(\Theta), m(\Theta)$ such that

$$\beta[\Theta] \quad = \quad \zeta^{k(\Theta)} \cdot y^{m(\Theta)} \cdot f(1/x; \Theta). \tag{10}$$

Here $f(1/x; \Theta) = \sum_{n=0}^{\infty} \frac{c_n(\Theta)}{p^{n+e(n)}} \cdot (1/x)^n$ is a series with $c_n \in \mathbb{Z}[\zeta]$ and $|c_n| < p^{m \cdot n}$ while $e(n) < n/(p-1)$. The idea for obtaining upper bounds consists in the following steps.

1. Select a subset $J_m \subset I$ such that $m = m(\Theta)$ is constant and *small* for all $\Theta \in J_m$. On the other hand the size $|J|$ should be *sufficiently large*.
2. Select a $J \subset J_m$ which is invariant under G, in the sense that $\Theta \in J \Rightarrow \sigma\Theta \in J$ for all $\sigma \in G$.
3. Let $\delta = \sum_{\Theta \in J} \lambda(\Theta)\beta[\Theta]$ be a linear combination with $\lambda(\Theta) \in \mathbb{Z}[\zeta]$.

4. Try to determine $\lambda(\Theta)$ such that $\mathbf{N}(\delta)$ is *small* but non null. Practically one wishes imposes conditions
$$\sum_{\Theta \in J} \lambda(\Theta) \cdot \zeta^{k(\Theta)} \cdot c_n(\Theta) = 0,$$
under some additional constraint which guarantees that $\delta \neq 0$. These are developed using (10)

The upper bounds in Theorem 3 are derived in this way, by using quadratic linear systems in 4. The use of under-determined systems can improve the bounds. The inhomogeneous condition $\delta \neq 0$ limits the efficacity of the approach. Lower bounds can be gained in some (lucky) cases by using the same argument locally. Thus for instance the case $x \equiv 0 \bmod p$ can be eliminated in (6).

Improvements of lower and/or upper bounds are called upon for a solution of the Nagell-Ljunggren equation.

References

[Be] Frits Beukers: *The Diophantine equation $Ax^p + By^q = Cz^r$*, Lectures held at Institut Henri Poincare, September 2004, http://www.math.uu.nl/people/beukers/

[BiH] Y. Bilu and G. Hanrot: *Solving superelliptic Diophantine equations by Baker's method*, Compositio Math. **112** (1998), pp. 273–312.
bibitem[BHM]BHM Y. Bugeaud, G. Hanrot and M. Mignotte: *Sur l'équation diophantienne $\frac{x^{n-1}}{x-1} = y^q$*, III, Proc. London. Math. Soc. **84** (2002), pp. 59-78.

[DG] H. Darmon and A. Granville: *On the Equation $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$*, Bull. London Math. Society, **27** (1995), no. 6, pp. 513- 543.

[Mi1] Preda Mihăilescu: *Class Number Conditions for the Diagonal Case of the Equation of Nagell – Ljunggren*, to appear.

[Mi2] Preda Mihăilescu: *New Bounds and Conditions for the Equation of Nagell – Ljunggren*, Journal of Number Theory, **Vol. 124** (2007) pp. 380-395.

[Mi3] Preda Mihăilescu: *A Cyclotomic Investigation of the Catalan – Fermat Conjecture*, Math ArXiv.

[Ri] P. Ribenboim: *Catalan's conjecture*, Academic Press, (1994).

Power integral bases for prime-power cyclotomic integer rings

Gabriele Ranieri

Let K be a number field and let $\mathcal{O}_K$ be its ring of integers. We say that K has a power basis if there exists $\alpha \in \mathcal{O}_K$ such that $\mathbb{Z}[\alpha] = \mathcal{O}_K$. It is rare (see [Gyo2]) for a number field to have a power basis. Neverthless if $K = \mathbb{Q}(\zeta_n)$, where n is a positive integer and ζ_n is a primitive nth root of unity, then $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$; hence all cyclotomic integer rings have a power basis.

Let $\alpha \in \mathbb{Z}[\zeta_n]$ such that $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta_n]$. We say that α is equivalent to $\beta \in \mathbb{Z}[\zeta_n]$ ($\alpha \sim \beta$) if and only if there exist an integer k and $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ such that:
$$\beta = \pm\sigma(\alpha) + k.$$
Then $\mathbb{Z}[\beta] = \mathbb{Z}[\zeta_n]$ and $\sim$ is an equivalence relation. It is an interesting problem to determine all the classes of generators of $\mathbb{Z}[\zeta_n]$. Gyory (see [Gyo1]) proves that there are only finitely many classes of generators of $\mathbb{Z}[\zeta_n]$ as to $\sim$.

Consider now the case $n = q$, where q is a power of the prime number $p \geq 2$. Bremner (see [Bre]) conjectures that there are only two classes of generators (as to $\sim$) of $\mathbb{Z}[\zeta_q]$: the class of ζ_q and the class of $1/(\zeta_q + 1)$ (actually in [Bre] Bremner only considers the case where $q = p$).

The first partial answer to Bremner's conjecture is given by Robertson (see [Rob]) who proves that if α is a generator of $\mathbb{Z}[\zeta_p]$ then either $\alpha \sim \zeta_p$ or $\alpha + \overline{\alpha}$ is an odd integer.

Afterwards Gaál and Robertson (see [Ga-Ro]) prove this weak generalization of the previous result: let q be a power of a prime $p \geq 2$, let h_q^+ be the class number of $\mathbb{Q}(\zeta_q + \overline{\zeta_q})$ and let $\alpha \in \mathbb{Z}[\zeta_q]$ be a generator of $\mathbb{Z}[\zeta_q]$; then if $(h_q^+, p(p-1)/2) = 1$ either $\alpha \sim \zeta_q$ or $\alpha + \overline{\alpha}$ is an odd integer.

Extensions of Cohen-Lenstra heuristics suggest that for a given q it is very likely that $(h_q^+, p(p-1)/2) = 1$. Moreover the Vandiver's conjecture, which says that p does not divide h_p^+, implies that p does not divide h_q^+ (see [Was], Corollary 10.5). Neverthless we do not know the value of h_q^+ for q such that $\phi(q) > 66$. Therefore it is interesting to ask if it is possible to remove the hypothesis about h_q^+ in [Ga-Ro]. In my talk I show that the hypothesis can be removed; in other words I prove that if $\alpha \in \mathbb{Z}[\zeta_q]$ is a generator of $\mathbb{Z}[\zeta_q]$ then either $\alpha \sim \zeta_q$ or $\alpha + \overline{\alpha}$ is an odd integer (see [Ran]).

References

[Bre] A. Bremner, *On power bases in cyclotomic number fields*, J. of Number Theory **28**, 288-298 (1988).

[Ga-Ro] I. Gaál, L. Robertson, *Power integral bases in prime-power cyclotomic fields*, J. of Number Theory **120**, 372-384 (2006).

[Gyo1] K. Gyory, *Sur les polynômes à coefficients entiers et de discriminant donné*, Acta Arithmetica **23**, 419-426 (1973).

[Gyo2] K. Gyory, *Corps de nombres algébriques d'anneau d'entiers monogène*, in Séminaire Delange-Pisot-Poitou, n. 26, Paris 1978-1979.

[Ran] G. Ranieri, *Générateurs de l'anneau des entiers d'une extension cyclotomique*, J. of Number Theory, to appear.

[Rob] L. Robertson, *Power bases for cyclotomic integer rings*, J. of Number Theory **69**, 98-118 (1998).

[Was] L. C. Washinghton, *Introduction to cyclotomic fields*. 2nd ed. GTM 84. New York, NY: Springer. xiv, 1997.

Diophantine equations and point distributions

Robert Tichy

In the first part of the lecture we establish a law of the iterated logarithm for the discrepancy of sequences $(n_k x) \bmod 1$ where (n_k) is a sequence of integers satisfying a sub-Hadamard growth condition and such that one and four-term Diophantine equations in the variables n_k do not have too many solutions. A suitable class of such sequences is given by a multiplicative semigroup generated by two or more coprime positive integers, where the elements of the semigroup in increasing order form the sequence (n_k). The conditions are discussed, the probabilistic details

of the proof are based on martingale inequalities and chaining arguments. The diophantine tools are applications of the subset theorem to S-unit equations. In particular it is necessary to estimate the number of solutions of the Diophantine equation

$$an_\nu + bn_\mu = c.$$

As a corollary to our results, the asymptotic behavior of sums $\sum f(n_k x)$ is obtained. (Joint work with Istvan Berkes and Walter Philipp).

In the second part we studied the problem of representing an algebraic integer as as sum of units in a given number field. (This is a joint work with Volker Ziegler). By a recent result of Jarden and Narkiewicz the ring of algebraic integers in a given number field cannot be generated additively by a finite number of units. However, it is an open problem to determining all number fields such that any integer can be represented as a sum of units. For quadratic number fields this problem has been solved by various authors. Our main result is concerned with purely cubic number fields.

Theorem 1. *Let d be a cube-free integer and let $\mathcal{O}_d$ be the maximal order of $\mathbb{Q}(\sqrt[3]{d})$. The ring $\mathcal{O}_d$ is generated by its units if and only if d is square-free, $d \not\equiv \pm 1 \mod 9$ and $d = a^3 \pm 1$ for some integer a or $d = 28$.*

The proof is based on Thue-equations and classical results of Siegel and Delauny for equations $ax^n + by^n = c$ with at most one solution. Furthermore, involved computations using Gröbner basis techniques are used.

Exponents of Diophantine Approximation and transfer inequalities

Michel Laurent

We present new inequalities which refine the well-known Khintchine Transference Principle. Let n be a positive integer and let $\Theta = (\theta_1, \ldots, \theta_n)$ be a point in $\mathbf{R}^n$. We shall assume in all the forthcoming statements that the real numbers $1, \theta_1, \ldots, \theta_n$ are linearly independent over the field $\mathbf{Q}$ of rational numbers. Khintchine Transference Principle relates the measure of simultaneous rational approximation to the real numbers $\theta_1, \ldots, \theta_n$ with the measure of linear independence over $\mathbf{Q}$ of the numbers $1, \theta_1, \ldots, \theta_n$. Our purpose is to split Khintchine's inequalities into $n-1$ intermediate estimates involving n exponents

$$\omega_d(\Theta), \quad 0 \le d \le n-1,$$

which measure the sharpness of the approximation to the point Θ by rational linear varieties of dimension d. We shall also be concerned with exponents of *uniform* approximation (indicated by a hat) and their relations to the exponents $\omega_d(\Theta)$.

Let us now define algebraically the exponents $\omega_d(\Theta)$, as well as their uniform analogues $\hat{\omega}_d(\Theta)$. First, extend naturally the usual Euclidean norm $|\cdot|$ on $\mathbf{R}^{n+1}$ to the Grassmann algebra $\Lambda\mathbf{R}^{n+1}$. Put

$$\mathbf{y} = (1, \theta_1, \ldots, \theta_n) \in \mathbf{R}^{n+1} = \Lambda^1 \mathbf{R}^{n+1}.$$

Definitions. Let d be an integer with $0 \le d \le n-1$. We denote by $\omega_d(\Theta)$ the supremum of the real numbers ω for which there exist infinitely many integer decomposable multivectors $\mathbf{X} \in \Lambda^{d+1}(\mathbf{Z}^{n+1})$ such that

$$|\mathbf{y} \wedge \mathbf{X}| \le |\mathbf{X}|^{-\omega}.$$

We denote by $\hat{\omega}_d(\Theta)$ the supremum of the real numbers ω such that for all sufficiently large positive real number H, there exists a non-zero integer decomposable multivector $\mathbf{X} \in \Lambda^{d+1}(\mathbf{Z}^{n+1})$ satisfying

$$|\mathbf{X}| \le H \quad \text{and} \quad |\mathbf{y} \wedge \mathbf{X}| \le H^{-\omega}.$$

It is easily seen that the extremal exponents $\omega_0(\Theta)$ and $\omega_{n-1}(\Theta)$ coincide with the supremum of the real numbers ω for which there exist infinitely many integer $(n+1)$-tuples $(x_0, \dots, x_n)$ satisfying respectively the inequations

$$\max_{1\le i\le n} |x_0\theta_i - x_i| \le \Big(\max_{0\le i\le n} |x_i|\Big)^{-\omega} \quad \text{or} \quad |x_0 + x_1\theta_1 + \cdots + x_n\theta_n| \le \Big(\max_{0\le i\le n} |x_i|\Big)^{-\omega}.$$

Thus $\omega_0(\Theta)$ clearly measures the simultaneous approximation to $\theta_1, \dots, \theta_n$ by rational numbers, while $\omega_{n-1}(\Theta)$ stands for the usual measure of linear independence of $\theta_1, \dots, \theta_n$.

Theorem 1. *For any integer d with $1 \le d \le n-1$, we have the estimate*

$$\frac{d\,\omega_d(\Theta)}{\omega_d(\Theta) + d + 1} \le \omega_{d-1}(\Theta) \le \frac{(n-d)\omega_d(\Theta) - 1}{n - d + 1}.$$

Composing the preceding inequalities from $d = 1$ to $d = n-1$, we recover Khintchine Transference Principle which reads here as follows

$$\frac{\omega_{n-1}(\Theta)}{(n-1)\omega_{n-1}(\Theta) + n} \le \omega_0(\Theta) \le \frac{\omega_{n-1}(\Theta) - n + 1}{n}. \tag{1}$$

We refer to [4] for more details and for an alternative geometrical definition of the exponents $\omega_d(\Theta)$ in terms of distance between the point Θ and rational linear varieties lying in the projective space $\mathbf{P}^n(\mathbf{R})$. Transfer inequalities of that type were first investigated by Schmidt in [5].

As for the uniform exponents $\hat{\omega}_d(\Theta)$ and their relations with $\omega_d(\Theta)$, few things are known. The extremal exponents $\hat{\omega}_0(\Theta)$ and $\hat{\omega}_{n-1}(\Theta)$ were initially introduced and studied by Jarník's. We direct the reader to [1, 2] for a survey of his results. The two dimensional case is now fully understood.

Theorem 2. *Let $\Theta = (\theta_1, \theta_2)$ be a point in $\mathbf{R}^2$ with $1, \theta_1, \theta_2$ linearly independent over $\mathbf{Q}$. Put*

$$v = \omega_1(\Theta), \quad v' = \omega_0(\Theta), \quad w = \hat{\omega}_1(\Theta), \quad w' = \hat{\omega}_0(\Theta).$$

Then, the relations

$$2 \le w \le +\infty, \quad w' = 1 - \frac{1}{w}, \quad \frac{v(w-1)}{v+w} \le v' \le \frac{v - w + 1}{w}$$

hold. Conversely, for each quadruple (v, v', w, w') *in* $(\mathbf{R}_{>0} \cup \{+\infty\})^4$ *as above, there exists a point* Θ *in* $\mathbf{R}^2$ *such that*

$$v = \omega_1(\Theta), \quad v' = \omega_0(\Theta), \quad w = \hat{\omega}_1(\Theta), \quad w' = \hat{\omega}_0(\Theta).$$

Notice that our refined transfer inequalities

$$\frac{v(w-1)}{v+w} \leq v' \leq \frac{v-w+1}{w}$$

sharpen Khintchine Transference Principle (1) when $n = 2$, since $w \geq 2$. In dimension two, the uniform transfer linking w and w', is achieved by the remarkable Jarník's equation

$$w' = 1 - \frac{1}{w}.$$

We easily deduce from Theorem 2 the non trivial lower bounds

$$v \geq w^2 - w \quad \text{and} \quad v' \geq \frac{w'^2}{1-w'},$$

which were first established by Jarník. A proof of Theorem 2 is given in [3].

With regard to Theorems 1 and 2, we are naturally led to ask for an extension of Theorem 2 in any dimension.

Problem. Let n be an integer ≥ 2. Describe a complete set of equations and inequations linking the $2n$ exponents

$$\omega_d(\Theta), \hat{\omega}_d(\Theta), \quad 0 \leq d \leq n-1,$$

for a generic point $\Theta \in \mathbf{R}^n$.

A report on the above results may also be found in [6].

References

[1] Y. Bugeaud and M. Laurent, *On exponents of homogeneous and inhomogeneous Diophantine approximation*, Moscow Mathematical Journal, 5, 4 (2005), 747–766.

[2] Y. Bugeaud and M. Laurent, *On exponents of Diophantine Approximation*, to appear in the Proceedings of the trimester on Diophantine approximation, Publ. of the Ennio de Giorgi Math. Institute, Pisa. `http://xxx.lanl.gov/pdf/math.NT/0611354`

[3] M. Laurent, *Exponents of Diophantine Approximation in dimension two*, to appear in the Canad. Journal of Math.. `http://xxx.lanl.gov/pdf/math.NT/0611352`

[4] M. Laurent, *On transfer inequalities in Diophantine Approximation*, to appear. `http://xxx.lanl.gov/pdf/math.NT/0703146`

[5] W. Schmidt, *On heights of algebraic subspaces and Diophantine approximations*, Ann. Math. 85 (1967), 430–472.

[6] M. Waldschmidt, *Report on some recent progress in Diophantine approximation*, to appear. `http://www.math.jussieu.fr/miw/`

New transference ideas in the metrical theory of Diophantine approximation

Victor Beresnevich
(joint work with Sanju Velani)

For $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$ consider the system of inequalities

$$|qx_i - p_i| \ < \ \psi(q) \quad \text{with } (p_i, q) = 1 \quad \text{for all } i = \overline{1, n}, \tag{1}$$

where $(q, \mathbf{p}) = (q, p_1, \dots, p_n) \in \mathbb{N} \times \mathbb{Z}^n$. Given $\psi : [0, +\infty) \to [0, +\infty)$, define

$$\mathcal{S}_n(\psi) = \{\mathbf{x} \in [0,1]^n : (1) \text{ holds for infinitely many } (q, \mathbf{p}) \in \mathbb{N} \times \mathbb{Z}^n\}.$$

The measure theoretic description of $\mathcal{S}_n(\psi)$ goes back to Khintchine. In 1926 Khintchine proved a beautiful and simple criterion for the Lebesgue measure of $\mathcal{S}_n(\psi)$, in which this measure is either 0 or 1 depending on whether the sum $\sum_{q=1}^{\infty} \psi(q)^n$ converges or diverges. The only restriction on ψ imposed in Khintchine's theorem has been the assumption that ψ is monotonic. In an attempt to relax this monotonicity constrain Duffin and Schaeffer stated a conjecture about the measure of $\mathcal{S}_1(\psi)$ later generalised by Sprindzhuk to higher dimensions:

Conjecture 1. *Let φ be the Euler function. Then*

$$|\mathcal{S}_n(\psi)| = 1 \qquad \text{if} \qquad \sum_{q=1}^{\infty} (\varphi(q)\,\psi(q)/q)^n \ = \ \infty.$$

For $n > 1$ the conjecture has been proved by Pollington and Vaughan, but for $n = 1$ it remains one of the most profound open questions. Only several partial results are known in dimension 1 due to Gallagher, Erdös, Vaaler and others.

A more general and far more delicate is the theory of Hausdorff measures of $\mathcal{S}_n(\psi)$. This theory goes back to Jarnik who found an analogue of Khintchine's theorem, again under monotonicity constrains on ψ. Nothing has been known outside the case of monotonic ψ, in particular, about the following main problem that generalises the conjecture of Duffin and Schaeffer to Hausdorff measures:

Conjecture 2. *Let f be a dimension function, i.e. $f : [0, +\infty) \to [0, +\infty)$ is continuous, monotonic and $f(0) = 0$. Assume that $x^{-n} f(x)$ is monotonic. Let $\psi : \mathbb{N} \to [0, +\infty)$. Then the f-dimensional Hausdorff measure $\mathcal{H}^f$ of $\mathcal{S}_n(\psi)$ satisfies*

$$\mathcal{H}^f\left(\mathcal{S}_n(\psi)\right) = \mathcal{H}^f\left([0,1]^n\right) \qquad \text{if} \quad V_n^f(\psi) := \sum_{q=1}^{\infty} f\left(\frac{\psi(q)}{q}\right) \varphi(q)^n = \infty.$$

It is readily verified that if $V_n^f(\psi) < \infty$ then $\mathcal{H}^f\left(\mathcal{S}_n(\psi)\right) = 0$, thus in certain sense Conjecture 2 provides a complete metric theory of $\mathcal{S}_n(\psi)$. Clearly, Conjecture 2 contains Conjecture 1. Simply take $\mathcal{H}^f$ to be the Lebesgue measure. It turns out that the converse is also true so that the two conjectures are in fact equivalent:

Theorem 1 (Beresnevich & Velani [1])**.** *Conjecture* 1 $\iff$ *Conjecture* 2.

Because Conjecture 1 has been established for $n > 1$, Conjecture 2 is also true for any $n > 1$. And if the original one dimensional Duffin-Schaeffer conjecture was proved, its Hausdorff measure version would immediately follow. This at first surprising fact has recently been obtained as a part of a general technique developed in [1] that we have maned by Mass Transference Principle. The key statement is the following

Theorem 2 (Beresnevich & Velani [1]). *Let f be a dimension function such that $x^{-n}f(x)$ monotonically decreases. Let $\{B_i\}_i$ be a sequence of balls in $\mathbb{R}^n$ with the radii of B_i tending to 0. As usually $\limsup_{i\to\infty} B_i$ denotes the set $\cap_{j=1}^{\infty}\cup_{i\geq j} B_i$. We define the following transformation of balls:*

$$B \mapsto B^f \qquad \text{such that} \qquad B^f(\mathbf{x}, r) = B\big(\mathbf{x}, f(r)^{1/n}\big),$$

where $B(\mathbf{x}, r)$ is the ball centred at $\mathbf{x}$ of radius r. If $f(x) = x^s$ then we write B^s for B^f and $\mathcal{H}^s$ for $\mathcal{H}^f$. Thus $B^n = B$. Then, for any ball $B \subset \mathbb{R}^n$

$$\mathcal{H}^n\left(B \cap \limsup_{i\to\infty} B_i^f\right) = \mathcal{H}^n(B) \quad \Longrightarrow \quad \mathcal{H}^f\left(B \cap \limsup_{i\to\infty} B_i^n\right) = \mathcal{H}^f(B).$$

Because the Mass transference principle is insensitive to the nature of balls the applications comprise various types of Diophantine approximation, *e.g.* inhomogeneous approximation, approximation with restricted numerator and denominator, approximation by algebraic numbers, *etc.* The Mass transference principle also works in locally compact metric spaces (see [1] for an appropriate statement) and has been extended to the case which allows to consider Diophantine systems of linear forms [2]. So far there is no Mass transference technique developed to the very general framework introduced in [3].

References

[1] V. Beresnevich, S. Velani, *A Mass Transference Principle and the Duffin-Schaeffer conjecture for Hausdorff measures*, Annals of Math. 164, no. 3 (2006) 971–992.

[2] V. Beresnevich, S. Velani, *Schmidt's theorem, Hausdorff measures, and slicing*, Int. Math. Res. Not. 2006, Art. ID 48794, 24 pp.

[3] V. Beresnevich, D. Dickinson, S. Velani, *Measure theoretic laws for lim sup sets*, Mem. Amer. Math. Soc. 179 (2006), no. 846, 91 pp.

[4] A. Baker and W.M. Scmidt, *Diophantine approximation and Hausdorff dimension*, Proc. Lond. Math. Soc., (21) 1970, 1–11.

Khintchine's theorem for simultaneous Diophantine approximations in several metrics

Vasili Bernik
(joint work with Nataliya Budarina and Detta Dickinson)

Let $n \in \mathbb{Z}$, $n > 0$ be fixed,

$$P(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0,\ a_i \in \mathbb{Z},\quad 0 \le j \le n \tag{1}$$

be an integral polynomial of degree $\deg P \le n$ and

$$H = H(P) = \max_{1 \le j \le n} |a_j|$$

be the height of P. We will consider the problem on approximation of zero by the values $P(x)$, $P(z)$, $|P(w)|_p$, where $\bar{u} = (x, z, w) \in \mathbb{R} \times \mathbb{C} \times \mathbb{Q}_p$. Let $\mu_1(A)$ be the Lebesgue measure of a measurable set $A \subset \mathbb{R}$, $\mu_2(B)$ is the Lebesgue measure of a measurable set $B \subset \mathbb{C}$, $\mu_3(D)$ is the Haar measure of a measurable set $D \subset \mathbb{Q}_p$ and $\mu = \mu_1 \mu_2 \mu_3$.

Let $\Psi : \mathbb{N} \to [0, +\infty)$ be a monotonically decreasing function, $\bar{v} = (v_1, v_2, v_3)$ and $\bar{\lambda} = (\lambda_1, \lambda_2, \lambda_3)$ are the vectors with real positive coordinates. By $\mathcal{L}_n(\bar{v}, \bar{\lambda})$ we denote the set of triples from some parallelepiped $T = I \times K \times D$, where I is an interval in $\mathbb{R}$, K is a circle in $\mathbb{C}$, D is a cylinder in $\mathbb{Q}_p$, for which the system of inequalities

$$\begin{cases} |P(x)| < H^{-v_1} \Psi^{\lambda_1}(H), \\ |P(z)| < H^{-v_2} \Psi^{\lambda_2}(H), \\ |P(w)|_p < H^{-v_3} \Psi^{\lambda_3}(H) \end{cases} \tag{2}$$

has infinitely many solutions in polynomials $P(t)$ of the form (1).

If we take $\bar{v} = (n-1, -1, 0)$ and $\bar{\lambda} = (1, 0, 0)$ then the set $\mathcal{L}_n(\bar{v}, \bar{\lambda})$ essentially reduces to the real case, which goes back to a famous problem of Mahler settled by Sprindzhuk in 1964. In fact this problem corresponds to the choice of $\Psi(H) = H^{-1-\varepsilon}$ with $\varepsilon > 0$. In the case of general monotonic Ψ the corresponding problem has been posed by A. Baker. The solution has been given by Bernik in [1] in the case of convergence of the sum $\sum_H \Psi(H)$ and by Beresnevich in [2] in the case of divergence of the same sum. Various generalisations of the real case have been obtained for complex and p-adic case. The work [3] combines them altogether. The following two theorems are the key statements:

Theorem 1. *Assume that* $n \ge 3$ *and*

$$\begin{cases} v_1 + 2v_2 + v_3 = n - 3, \\ \lambda_1 + 2\lambda_2 + \lambda_3 = 1. \end{cases} \tag{3}$$

Then

$$\mu \mathcal{L}_n(\bar{v}, \bar{\lambda}) = 0$$

provided $\sum_{H=1}^{\infty} \Psi(H) < \infty$.

Theorem 2. *If* $v_1 = v_2 = \frac{n-4}{4}$, $v_3 = \frac{n}{4}$, $\lambda_j = \frac{1}{4}$, $1 \le j \le 3$. *Then*

$$\mu\mathcal{L}_n(\bar{v}, \bar{\lambda}) = \mu T$$

provided $\sum_{H=1}^{\infty} \Psi(H) = \infty$.

The key to establishing Theorem 1 is a very deep generalisation of Gelfond's lemma which relates the upper bounds for small values of two irreducible polynomials and the size of domain where these values are taken by these polynomials.

References

[1] V.I. Bernik, *On the exact order of approximation of zero by values of integral polynomials*, Acta Arithmetica, (53) 1989, 17–28.

[2] V.V. Beresnevich, *On approximation of real numbers by real algebraic numbers*, Acta Arithmetica, (90) 1999, no. 2, 97–112.

[3] V. Bernik, N. Budarina and D. Dickinson, *A Khintchine type theorem for combined Diophantine approximations with integral polnomials in several metrics*, Preprint.

Hypergeometrics and linear forms in zeta values

Christian Krattenthaler

(joint work with Tanguy Rivoal)

The determination of the arithmetic nature of values of the Riemann zeta function $\zeta(s) = \sum_{k=1}^{\infty} 1/k^s$ at odd values $s \ge 3$ is one of the most challenging problems in number theory. After Apéry's celebrated proof [2] of the irrationality of $\zeta(3)$, it took over twenty years until the second author proved that there are infinitely many irrational numbers among $\zeta(3), \zeta(5), \zeta(7), \zeta(9), \dots$, as well as the quantitative result that there is at least one irrational numbers among $\zeta(5), \zeta(7), \zeta(9), \dots, \zeta(21)$ (cf. [3, 8, 9, 10]). The latter result has since been improved by Zudilin [14] to the assertion that one of $\zeta(5), \zeta(7), \zeta(9), \zeta(11)$ is an irrational number. See [4] for a comprehensive survey of these developments.

All the results mentioned are achieved by constructing a sequence of hypergeometric series, $(S_n)_{n\ge 0}$ say, which is shown to equal a linear combination of 1 and values of the zeta function at odd integers ≥ 3, with rational numbers as coefficients. One then multiplies S_n by a number N_n which is big enough to cancel all the denominators in these coefficients. In that way, one obtains a sequence N_nS_n of linear combinations of 1 and values of the zeta function at odd integers ≥ 3, with *integer* coefficients. Subsequently, one has to bound the growth of the linear forms N_nS_n, and one has to find bounds for the growth of the coefficients of the linear forms, as n tends to ∞. Given that these bounds are good enough, one can apply Nesterenko's lemma [7] to find a lower bound on the dimension of the vector space over the rationals spanned by 1 and the zeta values which appear in the linear combinations. The application of Nesterenko's lenma is the more effective, the smaller the growth of the "denominators" N_n is.

In [9], Rivoal proposed a sequence of hypergeometric series, which would comprise all the constructions from [3, 8, 9, 10] as special cases. Namely, for positive integers A, B, C, r, with A pair and $0 \le 2Br < A$, let

$$S_n = n!^{A-2Br} \sum_{k=1}^{\infty} \frac{1}{C!} \frac{\partial^C}{\partial k^C} \left(\left(k + \frac{n}{2}\right) \frac{(k-rn)_{rn}^B (k+n+1)_{rn}^B}{(k)_{n+1}^A} \right).$$

By the usual procedure indicated above, one easily shows that

$$S_n = \kappa_0 + \kappa_{C+3}\zeta(C+3) + \kappa_{C+5}\zeta(C+5) + \cdots + \kappa_{A+C-1}\zeta(A+C-1),$$

where the coefficients κ_j are rational numbers with the property that $d_n^{A+C}\kappa_j$ is an integer for all j. Here, d_n denotes the least common multiple of the numbers $1, 2, \ldots, n$. However, computer experiments suggest that apparently d_n^{A+C-1} "suffices," that is, that already $d_n^{A+C-1}\kappa_j$ is an integer for all j. This is indeed (a special case of) our main result from [6, Théorème 1].

Theorem 1. *We have $d_n^{A-i-1}\kappa_{C+i} \in \mathbb{Z}$ for all $i \ge 1$ and $2d_n^{A+C-1}\kappa_0 \in \mathbb{Z}$.*

The monograph [6] contains in fact further results in this direction, plus refinements of Theorem 1, proving (among others) conjectures of Vasilyev from [11, 12] (by taking a free ride on Zudilin's observation [13] that Vasilyev's integrals equal very-well-poised hypergeometric series) and of Zudilin from [13]; see [6, Théorèmes 1–6].

All the theorems are proved by making use of identities for hypergeometric series, most prominently a thirty years old identity between a very-well-poised hypergeometric series and a multiple sum due to Andrews [1, Theorem 4], combined with a careful p-adic analysis of the resulting terms. The hypergeometric calculations have been carried out by relying heavily on the first author's *Mathematica* package HYP [5].

The "good" news is that, as a corollary, one can improve the second author's result from [10] to the result that one number out of $\zeta(5), \zeta(7), \zeta(9), \ldots, \zeta(19)$ is irrational. In view of Zudilin's result from [14] mentioned earlier, this is however at the same bad news, since it cannot improve upon his result. However, all of Zudilin's constructions from [13, 14] are as well based on very-well-poised hypergeometric series, so that our methods are fully applicable. It is very likely that a "denominator conjecture" holds as well for Zudilin's constructions. He has in fact worked out a precise denominator conjecture in [13] which would lead to the best known upper bound on the irrationality measure of $\zeta(4)$. We are convinced that our methods will in the end lead to a proof of this conjecture.

Acknowledgments. Research partially supported by the Austrian Science Foundation FWF, grant P12094-MAT, and by EC's IHRP Programme, grant HPRN-CT-2001-00272, "Algebraic Combinatorics in Europe"

References

[1] G. E. Andrews, *Problems and prospects for basic hypergeometric functions*, Theory and application of special functions, R. A. Askey, ed., Math. Res. Center, Univ. Wisconsin, Publ. No. 35, Academic Press, New York, pp. 191–224, 1975.

[2] R. Apéry, *Irrationalité de $\zeta(2)$ et $\zeta(3)$*, Astérisque **61** (1979), 11–13.
[3] K. Ball et T. Rivoal, *Irrationalité d'une infinité de valeurs de la fonction zêta aux entiers impairs*, Invent. Math. **146**.1 (2001), 193–207.
[4] S. Fischler, *Irrationalité de valeurs de zêta (d'après Apéry, Rivoal, ...)*, Séminaire Bourbaki 2002–2003, exposé no. 910, Astérisque **294** (2004), 27–62.
[5] C. Krattenthaler, *HYP and HYPQ — Mathematica packages for the manipulation of binomial sums and hypergeometric series respectively q-binomial sums and basic hypergeometric series*, J. Symbol. Comput. **20** (1995), 737–744.
[6] C. Krattenthaler et T. Rivoal, *Hypergéométrie et fonction zêta de Riemann*, Mem. Amer. Math. Soc. 186, no. 875, Providence, R. I., 2007, 87 pp.
[7] Yu. V. Nesterenko, *On the linear independence of numbers*, Vest. Mosk. Univ., Ser. I (1985), 46–54; English trans. in Mosc. Univ. Math. Bull. **40**.1 (1985), 69–74.
[8] T. Rivoal, *La fonction zêta de Riemann prend une infinité de valeurs irrationnelles aux entiers impairs*, C. R. Acad. Sci. Paris, Série I Math. **331**.4 (2000), 267–270.
[9] T. Rivoal, *Propriétés diophantiennes des valeurs de la fonction zêta de Riemann aux entiers impairs*, Ph.D. thesis, Université de Caen (2001).
[10] T. Rivoal, *Irrationalité d'au moins un des neuf nombres $\zeta(5)$, $\zeta(7)$, ..., $\zeta(21)$*, Acta Arith. **103**.2 (2002), 157–167.
[11] D. V. Vasilyev, *Some formulas for the Riemann zeta function at integer points*, Vestnik Moskov. Univ. Ser I Mat. Mekh. **51**.1 (1996), pp. 81–84, English trans. in Moscow Univ. Math. Bull. **51**.1 (1996), pp. 41–43.
[12] D. V. Vasilyev, *Approximations of zero by linear forms in values of the Riemann zeta-function*, Doklady Nat. Acad. Sci. Belarus **45**.5 (2001), 36–40 (in Russian). Extended version in English: *On small linear forms for the values of the Riemann zeta-function at odd points*, preprint no.1 (558), Nat. Acad. Sci. Belarus, Institute Math., Minsk (2001), 14 pages.
[13] W. Zudilin, *Well-poised hypergeometric service for diophantine problems of zeta values*, J. Théor. Nombres Bordeaux **15**.2 (2003), 593–626.
[14] W. Zudilin, *Arithmetic of linear forms involving odd zeta values*, J. Théor. Nombres Bordeaux **16** (2004), 251–291.

Linear independence of values of Tschakaloff series

Wadim Zudilin
(joint work with Keijo Väänänen)

The arithmetic properties of values of the Tschakaloff function

$$T_q(z) = \sum_{\nu=0}^{\infty} q^{-\nu(\nu+1)/2} z^\nu, \qquad |q| > 1,$$

have been investigated in many works. One of the open problems is to prove linear independence of values of $T_q(z)$ with different values of the parameter q. The only result obtained in this direction in [1] is very restrictive, and in the present paper we generalize it considerably.

Let $q \in \mathbb{Z} \setminus \{0, \pm 1\}$, and let $t_1, \dots, t_d$ be positive integers (not necessarily distinct). We will distinguish the following two cases:

(1) *all the numbers $\sqrt{t_i/t_j}$ for $i \neq j$ are irrational*, and
(2) *some of the numbers $\sqrt{t_i/t_j}$ are rational.*

We will say that an ordered pair of (real or complex) numbers β and $\widehat{\beta}$ *belongs to a rational exponent* $\gamma = m/n$ if there exist integers s and r such that $\widehat{\beta}^{ms}/\beta^{ns} = q^r$, i.e., if the numbers $\widehat{\beta}^{\gamma}/\beta$ and q are multiplicatively dependent.

Theorem 1. *Let $\beta_1, \dots, \beta_d$ be nonzero rationals. Then the numbers*

$$1,\ T_{q^{t_1}}(\beta_1),\ \dots,\ T_{q^{t_d}}(\beta_d)$$

are linearly independent over $\mathbb{Q}$ if case (1) *holds or in case* (2)*, for any $i \neq j$ such that $\sqrt{t_i/t_j} \in \mathbb{Q}$, the pair β_i, β_j does not belong to the exponent $\sqrt{t_i/t_j}$.*

As special cases of Theorem 1 we have, for example, the linear independence of $1, T_q(\beta_1), T_{q^2}(\beta_2)$ and $T_{q^3}(\beta_3)$ for all $\beta_1, \beta_2, \beta_3 \in \mathbb{Q}\setminus\{0\}$, or the linear independence of $1,\ T_q(\beta_1),\ T_{q^2}(\beta_2)$ and $T_{q^4}(\beta_3)$ for all $\beta_1, \beta_2, \beta_3 \in \mathbb{Q} \setminus \{0\}$ unless the numbers β_3^2/β_1 and q are multiplicatively dependent.

If $\beta_1 = \cdots = \beta_d$, Theorem 1 implies the following result.

Theorem 2. *Let $\beta \in \mathbb{Q} \setminus \{0\}$, and let the integers $t_1, \dots, t_d$ be distinct. Then the numbers*

$$1,\ T_{q^{t_1}}(\beta),\ \dots,\ T_{q^{t_d}}(\beta)$$

are linearly independent over $\mathbb{Q}$ if case (1) *holds or in case* (2) *the numbers β and q are multiplicatively independent.*

Our considerations imply also linear independence results for values of the theta series

$$\Theta(q^{-1}, z) = \sum_{\nu=-\infty}^{\infty} q^{-\nu^2} z^{\nu}$$

(cf. [1]) related to the Tschakaloff function by the equality

$$\Theta(q^{-1}, z) = T_{q^2}\Big(\frac{z}{q}\Big) + T_{q^2}\Big(\frac{1}{qz}\Big) - 1.$$

Theorem 3. *Let $\beta_1, \dots, \beta_d$ be nonzero rationals such that the two numbers β_i and q are multiplicatively independent for all i. Then the numbers*

$$1,\ \Theta(q^{-t_1}, \beta_1),\ \dots,\ \Theta(q^{-t_d}, \beta_d)$$

are linearly independent over $\mathbb{Q}$ if case (1) *holds or in case* (2)*, for any $i \neq j$ such that $\sqrt{t_i/t_j} \in \mathbb{Q}$, any of the pairs β_i, β_j and β_i^{-1}, β_j does not belong to the exponent $\sqrt{t_i/t_j}$.*

Theorem 4. *Let $\beta \in \mathbb{Q} \setminus \{0\}$ and q be multiplicatively independent, and let the integers $t_1, \dots, t_d$ be distinct. Then the numbers*

$$1,\ \Theta(q^{-t_1}, \beta),\ \dots,\ \Theta(q^{-t_d}, \beta)$$

are linearly independent over $\mathbb{Q}$.

Our theorems remain valid if we replace $\mathbb{Q}$ by an imaginary quadratic field $\mathcal{I}$ and $\mathbb{Z}$ by the ring of integers of $\mathcal{I}$. We also stress that, due to the quantitative character of the method used in our proof, it is possible to estimate from below linear forms with integer coefficients involving the numbers in question.

References

[1] M. Amou and K. Väänänen, *On linear independence of theta values*, Monatsh. Math. **144** (2005), no. 1, 1–11.

Lagrangian interpolation and zeta values

Tanguy Rivoal

Interpolation series theory (i.e., expansion of entire functions in series of polynomials where the roots of the polynomials belong to a fixed set of $\mathbb{C}$) played an important rôle in diophantine approximation at the beginning of the twentieth century. In particular, it was used by Pólya [6] when he proved that the function 2^z is the entire function of smallest growth which sends $\mathbb{N}$ in $\mathbb{Z}$. The transcendence of e^α for any algebraic number $\alpha \neq 0$ was also obtained by Siegel [8] by expanding $\exp(z)$ at suitable interpolation points.

Interpolation methods were crucial in Gel'fond's proof the transcendence of e^π (see [3]): this was a first step towards the proof of Hilbert's 7th problem that α^β is transcendental when α, β are algebraic numbers, with $\alpha \neq 0, 1$ and β irrational. He first expanded the entire function $\exp(\pi z)$ in interpolation series at interpolation points $(\alpha_n)_{n\geq 0}$ given by the gaußian integers ordered by increasing modulus and argument, without multiplicity: we have $e^{\pi z} = \sum_{n=0}^{\infty} A_n\, z(z-\alpha_1)\cdots(z-\alpha_{n-1})$ for all $z \in \mathbb{C}$, where the coefficients A_n are given by a certain complex integral. By the residue theorem, we obtain

$$A_n = \sum_{k=0}^{n} \frac{e^{\pi\alpha_k}}{\prod_{\substack{0\leq j\leq n\\ j\neq k}}(\alpha_k-\alpha_j)} = \sum_{k=0}^{n} \frac{e^{\pi\alpha_k}}{\omega_{n,k}} = P_n(e^\pi),$$

where $P_n(X) \in \mathbb{Q}(i)[X, 1/X]$ is of degree $\sqrt{n/\pi} + o(\sqrt{n})$ in X and $1/X$. Gel'fond then proved the following results:

1) The number $P_n(e^\pi)$ is non zero for infinitely many n because $\exp(\pi z)$ is not a polynomial.

2) There exists $\Omega_n \in \mathbb{Q}(i)$ such that $\Omega_n P_n(e^\pi) \in \mathbb{Z}[i][e^\pi, e^{-\pi}]$ and the height H_n of the Laurent polynomial $\Omega_n P_n(X)$ is bounded by $e^{\mathcal{O}(n)}$.

3) We have $\Omega_n P_n(e^\pi) \ll \exp(-n\log(n) + \mathcal{O}(n))$.

The conclusion follows by standard arguments. Despite some works by Boehle [2], Kuzmin [4] and Siegel [8] for example, interpolation methods were replaced by more powerful (and less explicit) methods based on auxiliary functions contructed thanks to Siegel's lemma.

The aim of my talk during the Oberwolfach meeting was to report on my recent work [7], in which I show how another kind of interpolation process can be used in irrationality theory. More precisely, I show that the irrationality of $\log(2), \zeta(2)$ and $\zeta(3)$ (Apéry's theorem [1]) can be obtained by expanding the Hurwitz zeta function $\zeta(s,z) = \sum_{k=1}^{\infty} 1/(k+z)^s$ or related functions in interpolation series of rational functions (not only polynomials). Such an interpolation process was first studied by René Lagrange [5] in 1935 when the degree of the numerators and

denominators of the rational summands are essentially equal. For example, using certain of his formulae, I proved the following:

Theorem 1 (Rivoal, 2006). *For all $z \in \mathbb{C} \setminus \{-1, -2, \ldots\}$, we have that*

$$\zeta(2,z) = \sum_{n=0}^{\infty} A_{2n} \frac{(z-n+1)_n^2}{(z+1)_n^2} + \sum_{n=0}^{\infty} A_{2n+1} \frac{(z-n+1)_n^2}{(z+1)_n^2} \frac{z-n}{z+n+1},$$

where $A_0 = \zeta(2)$ and, for all $n \geq 0$,

$$A_{2n+1} = \frac{2n+1}{2\pi i} \int_{\mathcal{C}_n} \frac{(x+1)_n^2}{(x-n)_{n+1}^2} \zeta(2,x)\,\mathrm{d}x \in \mathbb{Q}\zeta(3) + \mathbb{Q}$$

and

$$A_{2n+2} = \frac{2n+2}{2\pi i} \int_{\mathcal{C}_n} \frac{(x+1)_n^2}{(x-n)_{n+1}^2} \frac{x+n+1}{x-n-1} \zeta(2,x)\,\mathrm{d}x \in \mathbb{Q}\zeta(3) + \mathbb{Q}.$$

The curve $\mathcal{C}_n$ encloses the points $0, 1, \ldots, n$ but none of the poles of $\zeta(2,z)$.

(By definition, $(u)_0 = 1$ and $(u)_m = u(u+1)\cdots(u+m-1)$ for $m \geq 1$.) The irrationality of $\zeta(3)$ is a corollary of this theorem. Indeed, by the residue theorem, it is easy to compute explicitely the coefficient A_n and to deduce that

$$d_n^3 A_n = u_n \zeta(3) - v_n \in \mathbb{Z}\zeta(3) + \mathbb{Z}$$

where $d_n = \operatorname{lcm}(1, 2, \ldots, n)$. Furthermore, from the integral representation of A_n, we obtain that

$$\limsup_{n \to +\infty} (d_n^3 A_n)^{1/n} \leq e^3(\sqrt{2}-1)^4 < 1.$$

Since $\zeta(2,z)$ is not a rational function of z, we necessarily have $A_n \neq 0$ for infinitely many n and the irrationality of $\zeta(3)$ is proved.

Similarly, the irrationality of $\log(2)$ can be deduced from the following result. Let

$$\widetilde{\zeta}(1,z) = \sum_{n=1}^{\infty} \frac{(-1)^n}{n+z}.$$

Theorem 2 (Rivoal, 2006). *For all $z \in \mathbb{C} \setminus \{-1, -2, \ldots\}$, we have*

$$\widetilde{\zeta}(1,z) = \sum_{n=1}^{\infty} A_n \frac{(z-n+2)_{n-1}}{(z+1)_n} \tag{1}$$

where, for all $n \geq 0$,

$$A_{n+1} = \frac{2n+1}{2\pi i} \int_{\mathcal{C}_n} \frac{(x+1)_n}{(x-n)_{n+1}} \widetilde{\zeta}(1,x)\,\mathrm{d}x \in \mathbb{Q}\log(2) + \mathbb{Q}.$$

The curve $\mathcal{C}_n$ encloses the points $0, 1, \ldots, n$ but none of the poles of $\widetilde{\zeta}(1,z)$.

I don't know if it is possible to obtain the irrationality of $\zeta(2)$ by means of R. Lagrange's interpolation. Instead, I found new interpolation formulae which enabled me to use rational functions with unequal degrees for the numerators and denominators. The irrationality of $\zeta(2)$ is then a consequence of the following theorem. By a slight abuse of notations, let

$$\zeta(1,z)=\sum_{n=1}^{\infty}\left(\frac{1}{n}-\frac{1}{n+z}\right).$$

Theorem 3 (Rivoal, 2006)**.** *For all $z\in\mathbb{C}\setminus\{-1,-2,\ldots\}$, we have*

$$\zeta(1,z)=\sum_{n=0}^{\infty}A_n\,\frac{(z-n+1)_n^2}{(z+1)_n}+\sum_{n=0}^{\infty}B_n\,\frac{(z-n+1)_n^2}{(z+1)_n}\,\frac{z-n}{z+n+1}$$

where $A_0=B_0=0$ and, for all $n\geq 1$,

$$A_n=\frac{1}{2\pi i}\int_{\mathcal{C}_n}\frac{(x+1)_n(x-n)}{(x-n)_{n+1}^2}\,\zeta(1,x)\,\mathrm{d}x\in\mathbb{Q}\zeta(2)+\mathbb{Q}$$

and

$$B_n=\frac{2n}{2\pi i}\int_{\mathcal{C}_n}\frac{(x+1)_n}{(x-n)_{n+1}^2}\,\zeta(1,x)\,\mathrm{d}x\in\mathbb{Q}\zeta(2)+\mathbb{Q}.$$

The curve $\mathcal{C}_n$ encloses the points $0,1,\ldots,n$ but none of the poles of $\zeta(1,z)$.

Bibliographie

[1] R. Apéry, *Irrationalité de $\zeta(2)$ et $\zeta(3)$*, Astérisque **61** (1979), 11–13.

[2] K. Boehle, *Über die Transzendenz von Potenzen mit algebraischen Exponenten (Verallgemeinerung eines Satzes von A. Gelfond)*, Math. Ann. **108** (1933), 56–74.

[3] A. O. Gel'fond, *Sur les nombres transcendants*, C. R. Acad. Sci. de Paris **189** (1929), 1224–1226.

[4] R. O. Kuzmin, *On a new class of transcendental numbers*, en russe, Izv. Akad. Nauk SSSR 3 (1930), 583–597.

[5] R. Lagrange, *Mémoire sur les séries d'interpolation*, Acta Math. **64** (1935), 1–80.

[6] G. Pólya, *Über ganzwertige ganze Funktionen*, Palermo Rend. **40** (1916), 1–16 (1916).

[7] T. Rivoal, Applications arithmétiques de l'interpolation lagrangienne, Preprint (2006), 24 pages, submitted for publication.

[8] C. Siegel, *Über die Perioden elliptischer Funktionen*, J. reine angew. Math. **167** (1932), 62–69.

Multidimensional integrals over the unit hypercube representing linear forms in zeta-values

Carlo Viola

(joint work with Georges Rhin)

Since Rivoal's theorem [1], [5] on the existence of infinitely many irrational values of the Riemann zeta-function at odd positive integers, the arithmetical study of $\mathbb{Q}$-linear forms in the values of the zeta-function at positive integers aroused the interest of several authors. The main techniques employed are the study of multiple hypergeometric and polylogarithmic series, and the arithmetical study of multiple

integrals of suitable rational functions over the unit hypercube. Concerning the latter, of special interest are (i) the Beukers-type multiple integrals:

$$B_n := \int\limits_{(0,1)^n} \frac{X_1^{a_1}(1-X_1)^{b_1}\dots X_n^{a_n}(1-X_n)^{b_n}}{(1-(1-X_1\dots X_{n-1})X_n)^{b_n+a_1-c_1}} \; \frac{\mathrm{d}X_1\dots\mathrm{d}X_n}{1-(1-X_1\dots X_{n-1})X_n},$$

where (to ensure convergence of B_n) $a_1,\dots,a_n$; $b_1,\dots,b_n$; c_1 are any non-negative integers such that

$$\begin{aligned} &c_2 := a_2 + c_1 - a_1,\\ &c_3 := a_3 + c_2 - a_2,\\ &\quad\dots\dots\dots\\ &c_{n-1} := a_{n-1} + c_{n-2} - a_{n-2} \end{aligned} \tag{1}$$

are also non-negative, and (ii) the Sorokin-type multiple integrals:

$$S_n := \int\limits_{(0,1)^n} \frac{x_1^{b_n}(1-x_1)^{a_{n-1}}\, x_2^{c_{n-1}}(1-x_2)^{b_{n-1}}\dots x_n^{c_1}(1-x_n)^{b_1}}{(1-x_1x_2)^{a_{n-1}+b_{n-1}-a_{n-2}}\dots(1-x_1\dots x_{n-1})^{a_2+b_2-a_1}(1-x_1\dots x_n)^{a_1+b_1-a_n}} \times \frac{\mathrm{d}x_1\dots\mathrm{d}x_n}{(1-x_1x_2)\dots(1-x_1\dots x_n)}$$

where the exponents satisfy the constraints (1).

In [4] we prove that

$$B_n = S_n,$$

using as a change of variables the birational transformation

$$\eta_n : (x_1,\dots,x_n) \longmapsto (X_1,\dots,X_n)$$

defined by the equations

$$\eta_n : \begin{cases} X_1 \;=\; \dfrac{(1-x_1\dots x_{n-1})x_n}{1-x_1\dots x_n}\\ X_2 \;=\; \dfrac{(1-x_1\dots x_{n-2})x_{n-1}}{1-x_1\dots x_{n-1}}\\ \quad\dots\dots\dots\dots\dots\\ X_{n-1} \;=\; \dfrac{(1-x_1)x_2}{1-x_1x_2}\\ X_n \;=\; 1-x_1\dots x_n. \end{cases}$$

It is easily seen that η_n is a one-to-one mapping of the open unit hypercube $(0,1)^n$ onto $(0,1)^n$, and that η_n is a solution to the partial differential equation

$$\frac{\mathrm{d}X_1\dots\mathrm{d}X_n}{1-(1-X_1\dots X_{n-1})X_n} \;=\; (-1)^{[n/2]+1}\,\frac{\mathrm{d}x_1\dots\mathrm{d}x_n}{(1-x_1x_2)\dots(1-x_1\dots x_n)}\,.$$

Using the equality of B_n and S_n, we also prove that

$$(2) \quad B_n = S_n = A_1 + A_2\zeta(2) + A_3\zeta(3) + \ldots + A_{n-1}\zeta(n-1) + A_n(n-1)\zeta(n)$$

with $A_1, A_2, \ldots, A_{n-1} \in \mathbb{Q},\ A_n \in \mathbb{Z}$. On the other hand, as was shown in a recent paper by Cresson, Fischler and Rivoal [2], more general Sorokin-type multiple integrals are $\mathbb{Q}$-linear combinations of polyzeta-values. Thus our result (2) shows that (1) are natural constraints for S_n, since they make S_n rid of polyzeta-values.

The representation (2) for B_n:

$$B_n = A_1 + A_2\zeta(2) + A_3\zeta(3) + \ldots + A_{n-1}\zeta(n-1) + A_n(n-1)\zeta(n)$$

can also be obtained as a special case of some formulae of Nesterenko [3] relating multiple integrals over the unit hypercube with complex integrals of Mellin-Barnes type and with linear forms in polylogarithms.

References

[1] K. Ball and T. Rivoal, *Irrationalité d'une infinité de valeurs de la fonction zêta aux entiers impairs*, Invent. Math. 146 (2001), 193-207.

[2] J. Cresson, S. Fischler and T. Rivoal, *Séries hypergéométriques multiples et polyzêtas*, Bull. Soc. Math. France, to appear.

[3] Yu. V. Nesterenko, *Integral identities and constructions of approximations to zeta-values*, J. Théor. Nombres Bordeaux 15 (2003), 535-550.

[4] G. Rhin and C. Viola, *Multiple integrals and linear forms in zeta-values*, to appear.

[5] T. Rivoal, *La fonction zêta de Riemann prend une infinité de valeurs irrationnelles aux entiers impairs*, C. R. Acad. Sci. Paris, Sér. I Math., 331 (2000), 267-270.

On a problem of Diophantus and Euler

Clemens Fuchs

Diophantus of Alexandria was interested in finding sets of (rational) numbers with the property that the product of any two of its distinct elements plus their sum is a perfect square. He gave the examples $\{4, 9, 28\}, \{\frac{3}{10}, \frac{21}{5}, \frac{7}{10}\}$. Euler gave an example of a set consisting of four rational numbers with this property, namely $\{\frac{5}{2}, \frac{9}{56}, \frac{9}{224}, \frac{65}{224}\}$. He asked the following:

> **Euler's question**: Is there a set consisting of four positive integers and the property that the product of any two distinct elements plus their sum is a perfect square, i.e. $\exists \mathcal{D} \subseteq \mathbb{Z}_{>0}$ such that for all $x, y \in \mathcal{D}, x \neq y : xy + x + y$ is always a perfect square?

It is interesting to observe that $xy + x + y = (x + 1)(y + 1) - 1$ and therefore we may equivalently ask for sets of integers larger than 1 with the property that the product of any two distinct elements decreased by 1 is a perfect square. This is related to another problem in which already Diophantus was interested in (for a general account on this see [Dujella]'s m-tuple page).

Let us mention that there are infinitely many sets with three elements and the above property, e.g. $\{1, 2x^2 + 2x, 2x^2 + 6x + 4\}, \{x^2, (x + 1)^2, (2x + 1)^2 + 3\}$. But these sets cannot be extended to sets $\mathcal{D}$ sought by Euler at least under the

assumption $x \not\equiv 1$ modulo 4 in the first and $x \not\equiv 0$ modulo 4 in the second case (this was shown by [Brown]).

Recently jointly with A. Dujella we gave the answer to the question of Euler.

Theorem ([Dujella - F.])**.** *The answer to Euler's question is no.*

More generally, we can consider $\mathcal{D} \subseteq \mathbb{Z}$; but if there is one negative element in $\mathcal{D}$, then all have to be less then -1 and by changing all the signs simultaneously we get a set considered in the theorem. However, it is not natural to exclude zero from $\mathcal{D}$ and this leads to a much harder problem. If $0 \in \mathcal{D}$, then all elements are squares. Recently, we were able to prove the following

Theorem ([Dujella - Filipin - F.])**.** *There are at most finitely many sets $\mathcal{D}$ of four integers such that the product of any two distinct elements from this set plus their sum is a perfect square. Moreover,* $\max \mathcal{D} \leq 10^{10^{23}}$.

The open problem remains to calculate all the remaining possibilities, the conjecture being that there is no such set at all.

The method of proof can be outlined as follows: From the first theorem above we may assume that $\mathcal{D} = \{0, r^2, s^2, t^2\}$ with $0 < r < s < x$. We set $b-1 = r^2, c-1 = s^2$, then $r^2s^2 + r^2 + s^2 = bc - 1 = t^2$. Moreover $d-1 = x^2, bd-1 = y^2, cd-1 = z^2$ with $1 < b < c < d$. Now we describe all possible d's once we start with given fixed b and c and in this way we prove an absolute upper bound for d. Thus we have to consider the system of Pellian equations given by

$$z^2 - cx^2 = c - 1, bz^2 - cy^2 = c - b, y^2 - bx^2 = b - 1,$$

where each two have a variable in common. By using the theory of Pellian equations we reduce the problem to find $z = v_m = w_n$, where $v_0 = z_0, v_1 = (2c-1)z_0 + 2scx_0, v_{m+2} = (4c-2)v_{m+1} - v_m$ and $w_0 = z_1, w_1 = (2bc-1)z_1 + 2tcy_1, w_{n+2} = (4bc-2)w_{n+1} - w_n$ with $|x_0| < s, |y_1| < t, 0 < z_0, z_1 < c$.

Using the recurring relations one can show that, if $v_m = w_n$, then $z_0 = z_1, m \equiv n \mod 2, n \leq m \leq 2n$ and $m^2 z_0 + smx_0 \equiv bn^2 z_1 + tny_1$ modulo c. The last important relation implies that the sequences cannot have intersections for small indices and therefore we get $d > b^9$ (this was an essential conclusion in the proof in [Dujella - F.]).

To finish the proof we consider six different cases, namely $c > b^9, 11b^3 \leq c \leq b^9, b^3 < c < 11b^6, b^{1.1} < c \leq b^3, 3b < c \leq b^{1.1}$ and $c < 3b$, and in each case we first prove a lower bound for n in terms of a power of c. The case of medium size solutions (the range $b^{1.1} < c < b^3$) is most delicate and in fact this is the most important new part of the proof.

If $c \geq 11b^6$, then Bennett's theorem on simultaneous approximations of square roots which are close to 1 (in a slightly refined version for our context by [Fujita]) gives the result.

In all other cases we compare the lower bounds for n with upper bounds obtained by turning $v_m = w_n$ into a linear form in three logarithms and using Baker's theory (we used [Matveev]'s theorem) and in this way, finally, we conclude with $d \leq 10^{10^{23}}$.

References

[Brown] E. Brown, *Sets in which $xy + k$ is always a square*, Math. Comp. **45** (1985), 613-620.

[Dujella] A. Dujella, *Diophantine m-tuples page*, http://web.math.hr/∼duje/dtuples.html.

[Dujella - F.] A. Dujella and C. Fuchs, *Complete solution of a problem of Diophantus and Euler*, J. London Math. Soc. (2) **71** (2005), 33-52.

[Dujella - Filipin - F.] A. Dujella, A. Filipin, and C. Fuchs, *Effective solution of the $D(-1)$-quadruple conjecture*, to appear.

[Fujita] Y. Fujita, *The extendibility of $D(-1)$-triples $\{1, b, c\}$*, Publ. Math. Debrecen **70** (2007), 103-117.

[Matveev] E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic number. II*, Izv. Ross. Akad. Nauk. Ser. Math. **64** (2000), no. 6, 125-180 (in Russian).

Diophantine m-tuples and generalizations

Andrej Dujella

A set of m positive integers is called a Diophantine m-tuple if the product of its any two distinct elements increased by 1 is a perfect square. Diophantus himself found a set of four positive rationals with the above property, while the first Diophantine quadruple, the set $\{1, 3, 8, 120\}$, was found by Fermat. In 1969, Baker and Davenport proved that this particular quadruple cannot be extended to a Diophantine quintuple. A folklore conjecture is that there does not exist a Diophantine quintuple.

In 2004, we have proved that there does not exist a Diophantine sextuple and there are only finitely many Diophantine quintuples. However, the bounds for the size of the elements of a (hypothetical) Diophantine quintuple are huge (largest element is less than $10^{10^{26}}$), so the remaining cases cannot be checked on a computer. The stronger version of this conjecture states that if $\{a, b, c, d\}$ is a Diophantine quadruple and $d > \max\{a, b, c\}$, then $d = a + b + c + 2abc + 2\sqrt{(ab+1)(ac+1)(bc+1)}$. Diophantine quadruples of this form are called regular.

In our future attempt to prove the Diophantine quintuple conjecture, our strategy will be to consider two different cases, depending on whether the hypothetical quintuple extends a regular or irregular Diophantine quadruple. The problem of extension of given Diophantine triple to a quadruple leads to solving a system of Pellian equations, and this leads to finding the intersection of binary recursive sequences. By a precise analysis of the initial terms of these sequences, we would like to improve inequalities which have to be satisfied by irregular quadruples. At present, it is known that $d > c^3$, and we intend to prove something like $d > c^7$. Such an inequality will allow us to apply very useful results (e.g. a result due to Bennett) on simultaneous Diophantine approximation of algebraic number close to

1. For the proof of extendibility of regular Diophantine quadruples, we intend to improve the congruence method, which is used to obtain lower bounds for solutions of the system of Pellian equations. We will again distinguish two cases depending of the form of the third element in the quadruple (one case is $c = a+b+2\sqrt{ab+1}$). In order to obtain upper bounds for solutions, we will use recent results, due to Matveev and Mignotte, on linear forms in logarithms of three algebraic numbers. The last step in the proof will certainly include an extensive verification on computers. Namely, we will have to check, by applying Baker-Davenport reduction method, that large (but hopefully reasonable) number of systems of Pellian equations have only trivial solutions. The proposed methods and steps of the proof have been recently tested, in the joint work with Yann Bugeaud and Maurice Mignotte, on the family of Diophantine triples $\{k-1, k+1, 16k^3-4k\}$, and we were able to prove that for this family the strong conjecture of unique extension to a Diophantine quadruple is valid.

Concerning rational Diophantine m-tuples, it is expected that there exist an absolute upper bound for their size. Such a result will follow from the Lang conjecture on varieties of general type. Very related problem is to find an upper bound M_n for the size of $D(n)$-tuples (for given non-zero integer n), i.e. sets of positive integers with property that $xy+n$ is perfect square for all of its distinct elements x, y. Again, the Lang conjecture implies that there exist an absolute upper bound for M_n (independent on n). However, at present, the best known upper bounds [Dujella, 2004] are of the shape $M_n < c \log |n|$. Recently, in our joint paper with Florian Luca, we were able to obtain an absolute upper bound for M_p, where p is a prime. Let us mention that several examples of rational Diophantine sextuples are known [Gibbs, 1999-2006], but it is not know whether there exist infinitely many such sextuples.

An interesting open question arises even when we consider the existence of quadruples. Namely, we stated the following conjecture: if n is not a perfect square, then there exist only finitely many $D(n)$-quadruples. It is very easy to verify the conjecture in case $n \equiv 2 \pmod 4$ (then there does not exist a $D(n)$-quadruple [Brown, 1984]), and recently, in the joint work with Clemens Fuchs and Alan Filipin, we have proved this conjecture in cases $n = -1$ and $n = -4$.

Quartic Diophantine Equations : the work of Akhtari

Michael Bennett

Over a period of nearly forty years, Wilhelm Ljunggren derived a number of remarkable sharp bounds for the number of solutions to various quartic Diophantine equations, particularly those of the shape

$$aX^4 - bY^2 = \pm 1, \tag{1}$$

typically via application of Skolem's p-adic method (some of the more sophisticated of Ljunggren's work essentially represents the earliest use of what would nowadays be termed "elliptic Chabauty techniques") . In recent years, there has

been renewed interest in Ljunggren's work (and quite a bit if recent progress on such equations). For example, using lower bounds for linear forms in logarithms, together with an assortment of elementary arguments, Walsh and I showed that the equation

$$aX^4 - bY^2 = 1 \tag{2}$$

has at most one solution in positive integers X and Y, when a is an integral square and b is a positive integer. On the other hand, for general a and b, there was, until recently, no absolute upper bound for the number of integral solutions to (2) available in the literature, unless one makes strong additional arithmetic assumptions. This lies in sharp contrast to the situation for the apparently similar equation

$$aX^4 - bY^2 = -1 \tag{3}$$

which Ljunggren was able to show to have at most two positive integral solutions, for arbitrary fixed a and b. Moreover, it appears that the techniques employed to treat equation (3) and, in special cases, (2), do not lead to results for (2) in general.

In this talk, I will survey recent work of Akhtari that rectifies this situation. Her main result is the following

Theorem 1. *Let a and b be positive integers. Then equation (2) has at most two solutions in positive integers (X, Y).*

This resolves a conjecture of Walsh. Since there are infinitely many pairs (a, b) for which two such solutions exist, this result is also best possible.

Akhtari's proof relies upon classical techniques of Thue from the theory of Diophantine approximation, applied to quartic Thue inequalities of the shape

$$|F(x, y)| \leq k,$$

where F is a binary quartic form. Specifically, she obtains sharp bounds for the number of solutions in integers to constrained inequalities of the shape

$$0 < P(x, y) = x^4 + 4tx^3y - 6tx^2y^2 - 4t^2xy^3 + t^2y^4 \leq t^2, \quad xy > 64t^3. \tag{4}$$

To reach such an inequality, she first uses properties of binary recurrence sequences to reduce the problem of bounding solutions to (2) to answering a like question for

$$(t+1)X^4 - tY^2 = 1,$$

which then can be shown, via elementary means, to give rise to solutions to (4).

To proceed, Akhtari defines $\xi = \xi(x, y)$ and $\eta = \eta(x, y)$ to be linear functions of (x, y) so that

$$\xi^4 = 4\,(\sqrt{-t} + 1)(x - \sqrt{-t}y)^4 \quad \text{and} \quad \eta^4 = 4\,(\sqrt{-t} - 1)(x + \sqrt{-t}y)^4.$$

We have

$$P(x, y) = \frac{1}{8}(\xi^4 - \eta^4)$$

and if (ξ, η) is a pair of such forms, then there are precisely three others with distinct ratios, say $(-\xi, \eta)$, $(i\xi, \eta)$ and $(-i\xi, \eta)$. Essentially, this diagonalizes the form $P(x, y)$, making possible direct application of classical results from the theory of Padé approximation to binomial functions. These are polynomials of degree r (or close to it), with rational coefficients, satisfying, say,

$$A_r(z) - (1-z)^{1/4} B_r(z) = z^{2r+1} F_r(z), \tag{5}$$

for a power series $F_r(z)$. For a fixed choice of ω, a fourth root of unity, and (ξ, η) a fixed pair of forms as above, set

$$z = 1 - \left(\frac{\eta(x,y)}{\xi(x,y)} \right)^4.$$

Akhtari shows that we may suppose, essentially without loss of generality, that

$$\left| \omega - \frac{\eta(x,y)}{\xi(x,y)} \right| < \frac{\pi}{12} |z|,$$

for each nontrivial solution (x, y) to (4).

Supposing that there are distinct coprime positive solutions (x_1, y_1) and (x_2, y_2) to inequality (4), each related to ω as above, and writing $\eta_i = \eta(x_i, y_i)$ and $\xi_i = \xi(x_i, y_i)$, the key to Akhtari's proof is to show that $|\eta_2|$ is arbitrarily large in size in comparison to $|\eta_1|$, contradicting the existence of 2 solutions corresponding to ω. By restricting to a single choice of ω, in a rather clever way, Akhtari proves Theorem 1.

The focal point of this part of the proof is (I'm oversimplifying things somewhat) to consider the complex sequences Σ_r given by

$$\Sigma_r = \frac{\eta_2}{\xi_2} A_r(z_1) - (-1)^r \frac{\eta_1}{\xi_1} B_r(z_1)$$

where $z_1 = 1 - \eta_1^4 / \xi_1^4$. Defining

$$\Lambda_r = \frac{\xi_1^{4r+1} \xi_2}{(-t-1)^{1/4}} \Sigma_r,$$

Akhtari shows that Λ_r is an integer in $\mathbb{Q}(\sqrt{-t})$; provided $\Sigma_r \neq 0$, this provides a lower bound upon its absolute value. Together with a modification of a "gap principle" of Evertse (to force $|\eta_1|$ and $|\eta_2|$ apart in size), this leads to the desired contradiction.

Apéry-like recursion and continued fraction for $\pi \coth \pi$

Kh. Hessami Pilehrood and T. Hessami Pilehrood

In 1929 A. O. Gel'fond proved that e^π is transcendental. This fact is a special case of Hilbert's seventh problem, which was solved independently by A. O. Gel'fond and Th. Schneider in 1934 (see [1], [2, Ch.3] for details). In 1932 Koksma and Popken [5] established the following quantitative refinement of Gel'fond's theorem.

Theorem. ([2, p.102]) *Let ε be an arbitrary positive number. Every polynomial $P \in \mathbb{Z}[x]$, $P(x) \not\equiv 0$, satisfies the inequality*

$$|P(e^{\pi})| \geq C \cdot H^{-(4+\varepsilon)\frac{\ln H}{\ln\ln H}},$$

where $H = \max(H(P), 3)$ and C is a positive constant depending only on $\deg P$ *and ε.*

However, it is unknown whether e^{π} is a Liouville number. This question has not yet been solved and conjecturally e^{π} is not a Liouville number (see [8, p.263]). Thus, the problem of constructing rational approximations to any number related to e^{π} represents an independent interest. In this presentation we deal with the number

$$\pi\coth\pi = \pi\cdot\frac{e^{\pi}+e^{-\pi}}{e^{\pi}-e^{-\pi}} = 1+\sum_{n=1}^{\infty}\frac{2}{n^2+1},$$

which is transcendental in view of algebraic independence of π and e^{π} due to Nesterenko's result [6]. Studying certain nearly-poised hypergeometric series with complex parameters, which give us linear forms in $\pi\coth\pi$ and 1 with rational coefficients and applying Zeilberger's algorithm of creative telescoping [7, Section 6] we obtain a second order difference equation for these forms and their coefficients. As a consequence, we find a new decomposition of $\pi\coth\pi$ into a continued fraction, which produces a rapidly convergent sequence of rational approximations to this number.

We consider the second-order difference equation

$$(n^2+2n+2)(n^2+2n+5)p(n)u_{n+1} - q(n)u_n - n^2(n^2+1)p(n+1)u_{n-1} = 0,$$

where

$$(1)\quad p(n) = 5n^2+2, \qquad q(n) = 55n^6+165n^5+242n^4+209n^3+127n^2+50n+12,$$

with the initial data

$$u_0 = 1,\ u_1 = \frac{3}{5}, \qquad v_0 = 1,\ v_1 = 2$$

and its two corresponding independent solutions u_n and v_n.

Theorem 1. *For every $n = 0, 1, 2, \ldots$, the numbers u_n and v_n are positive rationals such that*

$$\lim_{n\to\infty}\frac{v_n}{u_n} = \pi\coth\pi,$$

$$\lim_{n\to\infty}\Big|\pi\coth\pi - \frac{v_n}{u_n}\Big|^{\frac{1}{n}} = \Big(\frac{\sqrt{5}-1}{2}\Big)^{10} = \exp(-4.81211825\ldots),$$

$$\lim_{n\to\infty}u_n^{\frac{1}{n}} = \lim_{n\to\infty}v_n^{\frac{1}{n}} = \Big(\frac{\sqrt{5}+1}{2}\Big)^{5} = \exp(2.40605912\ldots).$$

The denominators u_n can be derived explicitly

$$u_n = \sum_{k=0}^{n} b_{k,n} = \prod_{j=1}^{n}\Big(\frac{j^2+1}{j^2+4}\Big)\cdot\sum_{k=0}^{n}(-1)^{n+k}\binom{n}{k}\prod_{j=1}^{k}\frac{(n+j)^2+1}{j^2+1}$$

and the numerators v_n are given by the formula

$$v_n = 2\sum_{k=0}^{n}\sum_{l=0}^{k}\frac{la_{k,n}+b_{k,n}}{l^2+1} - u_n,$$

where $a_{k,n}$ and $b_{k,n}$ are the real and imaginary parts of the complex number

$$i\binom{n}{k}\frac{(k+1+i)_n}{(1+2i)_k(1-2i)_{n-k}},$$

respectively. It can be shown (see [3, Lemma 3]) that the least common denominator of the numbers $a_{k,n}, b_{k,n}$, $k = 0, 1, \ldots, n$, is bounded by $e^{cn\log n}$ with some absolute constant c and therefore this construction doesn't allow one to obtain quantitative irrationality results.

If we consider $\frac{v_n}{u_n}$ as convergents of a continued fraction for $\pi\coth\pi$ and make an equivalence transformation of the fraction [4, Th.2.6], we get

Theorem 2. *The following continued fraction expansion is valid:*

$$\pi\coth\pi =$$

$$1+\frac{28}{q(0)}+\frac{20p(0)p(2)}{q(1)}+\cdots+\frac{n^2(n^2+1)^2(n^2+4)p(n-1)p(n+1)}{q(n)}+\cdots,$$

where the polynomials $p(n), q(n)$ are defined in (1).

Acknowledgements. This research was in part supported by grants from IPM: No. 85110020 (first author) and No. 85110021 (second author)

References

[1] N. I. Fel'dman, *Hilbert's seventh problem* [in Russian], Moscov. Gos. Univ., Moscow, 1982.
[2] N. I. Fel'dman, Yu. V. Nesterenko, *Number Theory IV. Transcendental numbers,* Encyclopaedia of Math. Sciences, V.44, Springer, 1998.
[3] A. I. Galočkin, *The arithmetic properties of the values of some entire hypergeometric functions* [in Russian], Sibirsk. Mat. Ž. **17** (1976), no.6, 1220-1235.
[4] W. B. Jones, W. J. Thron, *Continued fractions. Analytic number theory and applications,* Encyclopaedia Math. Appl. Section: Analysis, vol. 11, Addison-Wesley, London, 1980.
[5] J.F. Koksma, J. Popken, *Zur Transcendenz von e^π*, J. Reine Angew. Math. **168** (1932) 211-230.
[6] Yu. V. Nesterenko, *Modular functions and transcendence questions,* Mat. Sb. **187** (1996) no.9, 65-96.
[7] M. Petkovšek, H. S. Willf, and D. Zeilberger, $A = B$, A. K. Peters, Ltd., Wellesley, M. A., 1997.
[8] M. Waldschmidt, *Open diophantine problems,* Moscow Math. Journal **4** (2004) no.1, 245-305. math arXiv: NT/03124440

Hilbert's tenth problem: Diophantine equations from an algorithmical point of view

Yuri Matiyasevich

The talk contained short history of the negative solution of Hilbert's tenth problem and a survey of some other impossibility results about Diophantine equations. As an example we can state

Theorem (Matiyasevich [1]**).** *One can construct an exponential Diophantine equation*

$$E_{\mathrm{L}}(a, x_1, x_2, \ldots, x_m) \;=\; E_{\mathrm{R}}(a, x_1, x_2, \ldots, x_m) \tag{1}$$

with the following properties:

- *for every value of the parameter a, the equation* (1) *has at most one solution in $x_1, \ldots, x_m$;*
- *for every total (i.e., defined for all values of its argument) effectively computable function σ there is a value of a for which the equation* (1) *has a solution $x_1, \ldots, x_m$ such that $x_1 > \sigma(a)$.*

The left- and right-hand sides in (1) contains the exponentiation. It still remains an

Open problem. *To improve the above theorem to the case of genuine Diophantine equations (possibly under the weaker requirement of the existence of only finitely many solutions).*

References

[1] Yu. V. Matiyasevich, Existence of noneffectivizable estimates in the theory of exponential Diophantine equations (in Russian). *Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR (LOMI)*, **40** (1974), 77–93; Translated in: *Journal of Soviet Mathematics*, **8**(3) (1977), 299–311.

[2] Yu. V. Matiyasevich, *Desyataya Problema Gilberta.* Fizmatlit, Moscow, (1993). English translation: *Hilbert's Tenth Problem.* MIT Press, Cambridge (Massachusetts) London (1993). French translation: *Le dixième Problème de Hilbert*, Masson, Paris Milan Barselone (1995). URL: `http://logic.pdmi.ras.ru/~yumat/H10Pbook`.

[3] Yu. Matiyasevich, Hilbert's tenth problem: A two-way bridge between number theory and computer science. In C. S. Calude, editor, *People and Ideas in Theoretical Computer Science*, Springer series in discrete mathematics and theoretical computer science, pages 177–204. Springer-Verlag, Singapore, 1999.

[4] Hilbert's tenth problem: What was done and what is to be done. *Contemporary Mathematics* **270** (2000), 1–47.

[5] Yu. Matiyasevich, Hilbert's tenth problem and paradigms of computation, *Lecture Notes Computer Science*, **3526** (2005), 310–321.

[6] Yu. Matiyasevich, Computation Paradigms in the Light of Hilbert's Tenth Problem, to appear.

[7] A. Shlapentokh, *Hilbert's Tenth Problem. Diophantine Classes and Extensions to Global Fields*, Cambridge Univ. Press, Cambridge, New Your a.o., (2007).

Around a problem of Mahler and Mendès France

Boris Adamczewski

One motivation for this talk comes from a number theoretical problem concerning the expansion of algebraic numbers in integer bases. It appears at the end of a paper of Mendès France, but in conversation he attributes the paternity of this problem to Mahler. The problem reads as follows: for any non-eventually periodic binary sequence $(a_n)_{n\geq 0}$, prove that at least one of the two real numbers

$$\alpha = \sum_{n\geq 0} \frac{a_n}{2^n} \quad \text{and} \quad \beta = \sum_{n\geq 0} \frac{a_n}{3^n}$$

is transcendental. At first glance, this problem seems contrived, but behind it hides the more fundamental question of the structure of representations of real numbers in two mutliplicatively independent integer bases. Unfortunately, problems of this type are difficult and, up to now, it seems that no progress has been achieved towards this particular question.

However, when considering addition and multiplication without carry things become easier. In particular, we have a nice result of Christol, Kamae, Mendès France and Rauzy [4]: a sequence of coefficients represents two algebraic power series in distinct characteristics if and only if these power series are rational functions. In particular, Christol *et al.* give the following result, solving the positive characteristic analog of the problem.

Theorem 1 (Christol *et al.*)**.** *Let $(a_n)_{n\geq 0}$ be a binary sequence. Then, the formal power series*

$$f(t) = \sum_{n\geq 0} a_n t^n \in \mathbb{F}_2((t)) \quad \textit{and} \quad g(t) = \sum_{n\geq 0} a_n t^n \in \mathbb{F}_3((t))$$

are both algebraic (respectively over $\mathbb{F}_2(t)$ and $\mathbb{F}_3(t)$) if and only if they are rational functions.

As was remarked by Christol *et al.*, Theorem 1 is a straightforward consequence of two important results. On one side, Christol's theorem describes precisely in terms of automata the algebraic closure of $\mathbb{F}_q(t)$ in $\mathbb{F}_q((t))$ (q being a power of a prime p). On the other side, one finds Cobham's theorem proving that for multiplicatively independent positive integers k and l, a sequence that is both k- and l-automatic is eventually periodic.

In this talk, we will survey some results related to the positive characteristic, to the mixed charcteristic and to the p-adic counterparts of the problem of Mahler and Mendès France. These results involve tools from automa theory, combinaotrics on words and Diophantine approximation.

(i) Following [1], we will explain how to generalize Theorem 1 to the fields of generalized power series introduced by Hahn (and we will give some motivation for that). This work relies on the recent generalization of Christol's theorem obtained by Kedlaya [5].

(ii) We will also discuss the following solution to the mixed-characteristic analog of the Mahler–Mendès France problem.

Theorem 2. *Let p be a prime, $(a_n)_{n\geq 1}$ be an infinite sequence on $\{0,1,\dots,p-1\}$ and set*

$$\alpha = \sum_{n=1}^{+\infty} \frac{a_n}{p^n} \quad \textit{and} \quad f(t) = \sum_{n=1}^{+\infty} a_n t^n \in \mathbb{F}_p((t)).$$

Then, α and f are algebraic (resp. over $\mathbb{Q}$ and over $\mathbb{F}_p(t)$) if and only if both are rational.

This result (proved in [2]) relies on Chrisol's theorem and on a p-adic version of the subspace theorem.

(iii) The p-adic counterpart of the problem is raised in [3] and reads as follows.

Problem. Let p be a prime number, $(a_n)_{n\geq 1}$ be an infinite sequence on $\{0,1,\dots,p-1\}$, and set

$$\alpha = \sum_{n=1}^{+\infty} \frac{a_n}{p^n} \quad \textit{and} \quad \alpha_p = \sum_{n=1}^{+\infty} a_n p^n.$$

Then, prove that the real number α and the p-adic number α_p are algebraic if and only if both are rational.

In [3], we solve some particular instance of this problem, namely in the case where we can detect an excess of symmetry in the sequence $(a_n)_{n\geq 1}$. This result relies on the p-adic subspace theorem.

References

[1] B. Adamczewski & J. Bell, *Function fields in positive characteristic: expansions and Cobham's theorem*, J. Algebra, to appear.

[2] B. Adamczewski & Y. Bugeaud, *On the complexity of algeraic numbers I. Expansions in integer bases*, Annals of Math. 165 (2007), 547–565.

[3] B. Adamczewski & Y. Bugeaud, *Real and p-adic expansions involving symmetric patterns*, Int. Math. Res. Not. (2006), Article ID 75968, 17 pages.

[4] G. Christol, T. Kamae, M. Mendès France & G. Rauzy, *Suites algébriques, automates et substitutions*, Bull. Soc. Math. France 108 (1980), 401–419.

[5] K. Kedlaya, *Finite automata and algebraic extensions of function fields*, J. Théor. Nombres Bordeaux 18 (2006), 379–420.

Functional approximations of curves in projective spaces

Patrice Philippon

The approximation of transcendental objects by algebraic ones is an important tool in diophantine approximation, it reduces algebraic independence type properties to approximation ones. We will present results in the functional case when one approximates germs of transcendental functions (in a single variable) by algebraic functions. This has applications in the context of multiplicity estimates.

Let $\mathbf{k}$ be a commutative algebraically closed field and z a variable on this field. We denote $C := \mathbf{k}((z))$ and $\overline{C}$ an algebraic closure of C. For $\alpha, \beta \in \mathbf{P}_n(\overline{C})$ we define

$$\mathrm{Ord}_z(\alpha \wedge \beta) := \min_{0 \le i < j \le n} \mathrm{ord}_z(\alpha_i\beta_j - \alpha_j\beta_i) - \mathrm{ord}_z(\alpha) - \mathrm{ord}_z(\beta) \ ,$$

where ord_z stands for the extension to $\overline{C}$ of the order valuation of C.

One of our typical approximation result reads [2] :

Transference lemma – *Let $b \ge 2^{n-1}$, $\mu \ge n \ge 2$ and $\phi \in \mathbf{P}_n(C)$ such that $\phi_0 \ne 0$ et $\frac{\phi_1}{\phi_0} \in \mathbf{k}(z) \setminus \mathbf{k}$, if a non zero form $P \in \mathbf{k}[X_0, \ldots, X_n]$ satisfies $d^\circ P \ge 2(n+1)$ and*

$$\mathrm{ord}_z(P \circ \phi) - d^\circ P.\mathrm{ord}_z(\phi) > b d^\circ P^\mu \ ,$$

then there exists a cycle $Z = \{\alpha_1, \ldots, \alpha_D\} \subset \mathbf{P}_n(\overline{\mathbf{k}(z)})$ of dimension 0 and defined over $\mathbf{k}(z)$, contained in the set of zeros of P, satisfying

$$D = \deg(Z) \le b^{\frac{n-2}{n-1}} d^\circ P^{\frac{1+\mu(n-2)}{n-1}} \quad , \quad h(Z) \le h(\phi_0 : \phi_1) b^{\frac{n-2}{n-1}} d^\circ P^{\frac{1+\mu(n-2)}{n-1}}$$

and

$$\begin{aligned} \sum_{\alpha \in Z} \mathrm{Ord}_z(\alpha \wedge \phi) &> \frac{1}{4c_n} b^{\frac{1}{n-1}} \left(\frac{h(Z)}{h(\phi_0 : \phi_1)} + \deg(Z) \right) d^\circ P^{\frac{\mu-1}{n-1}} \\ &> \frac{1}{2c_n} b^{\frac{1}{1+\mu(n-2)}} \left(\frac{1}{2} \left(\frac{h(Z)}{h(\phi_0 : \phi_1)} + \deg(Z) \right) \right)^{\frac{\mu(n-1)}{1+\mu(n-2)}} \end{aligned}$$

The usual metric equivalent (for complex or p-adic numbers) of this lemma is still a conjecture, which has been proved only when $n \le 3$, *see* [1].

This lemma can be used in order to prove multiplicity estimates for families of series in one variable, satisfying a certain type of algebraic (functional or differential) equations [2].

References

[1] P. Philippon, *Approximations algébriques des points dans les espaces projectifs I*, J. Number Theory 81, 2000, 234-253.

[2] P. Philippon, *Approximations fonctionnelles des courbes des espaces projectifs*, manuscript, 22p.

Hilbert irreducibility theorem for linear algebraic groups

Pietro Corvaja

The celebrated Hilbert Irreducibility Theorem can be rephrased in the following way:

Theorem (HIT). *Let Y be an affine curve defined over $\mathbf{Q}$, not necessarely irreducible, $\pi : Y \to \mathbf{G}_a$ be a finite morphism. If every integer has a rational pre-image, i.e. $\pi(Y(\mathbf{Q})) \supset \mathbf{Z}$, then π admits a section (defined over $\mathbf{Q}$).*

Here $\mathbf{G}_a$ is the additive group, isomorphic as an algebraic variety to the affine line $\mathbf{A}^1$, and $\mathbf{Z}$ is the group of integers, which is a Zariski-dense subgroup of $\mathbf{G}_a$.

We consider natural generalizations to linear algebraic groups, not necessarily commutative. Using recent results of A. Ferretti and U. Zannier on diophantine equations involving linear recurrence sequences, we prove:

Main Theorem. *Let G be a connected linear algebraic group, defined over a number field k; let Y be an (affine) smooth algebraic variety, $\pi : Y \to G$ a finite map. Let $\Gamma \subset G(k)$ be a Zariski-dense subgroup. If $\pi(Y(k)) \supset \Gamma$ then there exists an irreducible component Y' of Y such that the map $\pi_{|Y'} : Y' \to G$ is unramified. In particular, Y' admits an algebraic group structure.*

This generalizes a result of P. Dèbes for the multiplicative group $\mathbf{G}_m$, which was obtained via Siegel's Theorem on integral points on curves.

As a corollary we obtain that no Zariski-dense subgroup of a simply connected (linear) algebraic group is thin.

A second corollary asserts that in every Zariski-dense subgroup of $\mathrm{GL}_n(k)$ there exist matrices whose characteristic polynomial is irreducible over k. As a very special case we obtain the following result, proved by J. Bernik:

Corollary. *Let $\Gamma \subset \mathrm{GL}_n(\mathbf{C})$ be a sub-semigroup. Suppose there exist a finitely generated field $k \subset \mathbf{C}$ containing the spectrum of every element of Γ. Then the subgroup generated by Γ contains a normal solvable subgroup of finite index.*

We shall also discuss some conjectural extensions of the above Main Theorem to semi-abelian varieties. We first recall the notion of S-integral point of a quasi projective variety. Given a finite set of places S of a number field k, a quasi-projective variety $V \subset \mathbf{P}_N$, let $D = \bar{V} \setminus V$ be its complement in the Zariski-closure $\bar{V}$ of V (so $D = \emptyset$ if V is projective). We say that a rational point $P \in V(k)$ is S-integral if for no prime ν outside S, the ν-reduction of P lies in D.

We propose the following

Conjecture. Let G be a semi-abelian variety defined over a number field k; let V be a smooth variety, $\pi : V \to G$ a finite morphism, all defined over k. If the set of S-integral points $V(\mathcal{O}_S)$ is Zariski-dense in V, then the morphism π is an unramified covering. In particular, V admits the structure of a semi-abelian variety such that π becomes an isogeny.

In the particular case $G = \mathbf{G}_m^n$ is a linear torus, this conjecture has been formulated by Zannier; it implies the (conjectural) finiteness of perfect squares of the form $1 + 2^a + 3^b$. In the particular case V is projective, it can be formulated as follows:
If the smooth projective variety V satifies $\dim \mathrm{Alb}(V) \geq \dim V$ *and V is not an abelian variety, then $V(k)$ is not Zariski-dense.*

Here $\mathrm{Alb}(V)$ denotes the Albanese variety of V. A famous theorem of Faltings implies the same conclusion under the hypothesis that $\dim \mathrm{Alb}(V) > \dim V$.

Almost integer-valued functions in characteristic p

Noriko Hirata-Kohno
(joint work with David Adam)

Let $f(z)$ be a complex entire function in one variable which satisfies $f(\mathbb{N}) \subset \mathbb{Z}$. A theorem of G. Pólya [8] assures that such function f is a polynomial if the order of exponential type $\overline{\lim}_{r\to+\infty} \frac{\log |f|_r}{r}$ is less than $\log 2$ (we denote $|f|_r = \sup_{|z|\leq r} |f(z)|$). Instead of the assumption $f(\mathbb{N}) \subset \mathbb{Z}$, we may consider functions not necessarily integer-valued on $\mathbb{N}$. In fact, Ch. Pisot proved [7] that an entire function on $\mathbb{C}$ taking values sufficiently near by integers on $\mathbb{N}$, is a polynomial whenever $\overline{\lim}_{r\to+\infty} \frac{\log |f|_r}{r} < \log 2$. The author gave an alternative proof [5] of Pisot's theorem by using transcendental method, so-called Schneider's method. Let us recall a simple corollary in [5]: let f be an entire function on $\mathbb{C}$ satisfying

$$\overline{\lim_{r\to+\infty}} \frac{\log |f|_r}{r} < \frac{1}{451}.$$

For all $n \in \mathbb{N}$, we denote by $||f(n)||$ the distance between $f(n)$ and the nearest integer, namely

$$||f(n)|| = \inf_{m\in\mathbb{Z}} |f(n) - m|.$$

Suppose

$$||f(n)|| < e^{-5n} \text{ for all } n \in \mathbb{N} \text{ sufficiently large.}$$

Then, f is a polynomial.

We remark that P. Stäckel [9] showed in 1894 an existence of an entire transcendental function taking algebraic values at all algebraic points. From his proof, we may also construct an example of an entire *transcendental* function F such that $F(\mathbb{N}) \subset \mathbb{Q}$ or $F(\mathbb{Z}) \subset \mathbb{Q}$ of arbitrary small order of exponential type. We then see that an analogy of Pólya's result does not hold in general for rational-valued functions on $\mathbb{N}$ or $\mathbb{Z}$ (*see also* [4]).

Now we present here a corresponding theorem in characteristic p. Let q be a power of a rational prime p, $\mathbb{F}_q$ be a finite field with q elements. Let $\mathbb{F}_q\left(\left(\frac{1}{T}\right)\right)$ be the field of Laurent series with coefficients in $\mathbb{F}_q$. This field is complete concerning with the norm "deg" induced by the degree with respect to T of a rational function in $\mathbb{F}_q(T)$. The completion denoted by $\mathcal{C}$ of the algebraic closure of $\mathbb{F}_q\left(\left(\frac{1}{T}\right)\right)$, is

again algebraically closed. The set $\mathcal{C}$ corresponds to $\mathbb{C}$ in characteristic 0. We continue denoting by deg the extension of the degree on $\mathcal{C}$.

An entire function f on $\mathcal{C}$ is a function

$$f(z) = \sum_{n\geq 0} a_n z^n \qquad \text{with } a_n \in \mathcal{C} \text{ for all } n \in \mathbb{N}$$

that converges for all $z \in \mathcal{C}$. For $r \in \mathbb{R}$, $r > 0$, we define $M(f, r)$ of f by

$$M(f, r) = \sup_{\deg(z)\leq r} \{\deg(f(z))\}.$$

D. Adam proved [1] the analogy of Pólya's theorem in characteristic p as follows: let f be an entire function on $\mathcal{C}$ such that

$$\overline{\lim_{r\to+\infty}} \frac{M(f, r)}{q^r} < \frac{1}{e \ln q} \qquad \text{and} \qquad f(\mathbb{F}_q[T]) \subset \mathbb{F}_q[T].$$

Then, f is a polynomial $\in \mathbb{F}_q(T)[z]$ and the bound $\frac{1}{e \ln q}$ is optimal.

Now let us mention our results. Let S be a subset of $\mathbb{F}_q[T]$. We put

$$\mathrm{Int}(S, \mathbb{F}_q[T]) = \{P \in \mathbb{F}_q(T)[z] \mid P(S) \subset \mathbb{F}_q[T]\}$$

and denote it by $\mathrm{Int}(\mathbb{F}_q[T])$ if $S = \mathbb{F}_q[T]$.

For a polynomial $H \in \mathbb{F}_q[T]$, which plays a role of an integer in the case of characteristic p, we put $||f(H)||$ the distance between $f(H)$ and the nearest element of $\mathbb{F}_q[T]$, *i. e.*

$$||f(H)|| = \inf_{Q\in\mathbb{F}_q[T]} \{\deg(f(H) - Q)\}.$$

When $||f(H)||$ is sufficiently small for all H of sufficiently large degree, we say that f is an almost integer-valued function.

If f is already a polynomial $\in \mathcal{C}[z]$ and almost integer-valued under a suitable condition on the speed, then it can be seen that f is indeed integer-valued, *i. e.* $P \in \mathrm{Int}(\mathbb{F}_q[T])$.

Now we show that an almost integer-valued entire function is a polynomial provided that the order of exponential type is controlled [2].

Theorem 1. *There exist two positive constants c_1 and c_2 that depend only on q satisfying the followings. Let f be an entire function on $\mathcal{C}$ which verifies the two conditions*

(1) $\overline{\lim_{r\to+\infty}} \dfrac{M(f, r)}{q^r} < c_1$

(2) $||f(H)|| < -c_2 q^{\deg(H)}$ *for all $H \in \mathbb{F}_q[T]$ of sufficiently large degree.*

Then $f \in \mathrm{Int}(\mathbb{F}_q[T])$.

We also get a version of result of Gel'fond, for such an almost integer-valued entire function, over the powers of a polynomial. Let $H \in \mathbb{F}_q[T]$ with $\deg H = h \geq 1$. Put $S = \{H^n \mid n \in \mathbb{Z},\ n \geq 0\}$.

Theorem 2. *There exist $c_3 > 0$ depending only on q and $c_4 > 0$ depending only on q and h, satisfying the followings. Let f be an entire function on $\mathcal{C}$ which verifies the two conditions*

(1) $M(f,r) \leq \dfrac{c_3}{h} r^2$

(2) $||f(H^n)|| \leq -c_4 n^2$ *for all $n \in \mathbb{N}$ sufficiently large.*

Then $f \in \mathrm{Int}(S, \mathbb{F}_q[T])$.

As seen before, it is sufficient to prove $f \in \mathcal{C}[z]$ to get the theorems.

Our proof is by means of Schneider's method and is based on Lemma 3, a residue formula with ultrametric Blashke factor for modified Schnirelmann integrals. Let f be an analytic function on $\overline{\Gamma} := \{z \in \mathcal{C} \mid \deg(z) \leq R\}$. Schnirelmann integral of f over $\Gamma := \{z \in \mathcal{C} \mid \deg(z) = R\}$ is defined by

$$\int_\Gamma f(z)dz = \lim_{\substack{n \to +\infty \\ p \not| n}} \frac{1}{n} \sum_{\xi^n = 1} f(\xi\gamma)$$

where γ denotes any element of Γ (Schnirelmann integral is originally defined on p-adic number field [6]).

Lemma 3. *Let f be an analytic function on $\overline{\Gamma}$ and $\xi_0, \xi_1, \cdots, \xi_l$ be distinct points in $\Gamma^\circ := \{z \in \mathcal{C} \mid \deg(z) < R\}$. Then we have*

$$\deg(f(\xi_0)) \leq \max\{G_1, G_2\}$$

where

$$G_1 = M(f,R) - lR + \sum_{n=1}^{l} \deg(\xi_0 - \xi_n),$$

$$G_2 = \max_{1 \leq n \leq l} \left\{ \deg(f(\xi_n)) + \sum_{\substack{k=1 \\ k \neq n}}^{l} \deg\left(\frac{\xi_0 - \xi_k}{\xi_n - \xi_k}\right) \right\}.$$

References

[1] D. Adam, *Car-Pólya and Gel'fond's theorems for $\mathbb{F}_q[T]$*, Acta Arith. **115. 3** (2004), 287–303.

[2] D. Adam & N. Hirata-Kohno, *Almost integer-valued functions in positive characteristic*, preprint.

[3] P. J. Cahen, J. L. Chabert, *Integer valued polynomials*, Mathematical Survey and Monographs **48**, American Mathematical Society, Providence (1997).

[4] F. Gramain, *Fonctions entières arithmetiques: un aperçu historique*, Pub. IRMA - Lille **VI**, Fasc. 2 (1984), n^o 1.

[5] N. Hirata, *Dépendance linéaires de fonctions arithmétiques et presque arithmétiques*, Publ. Math. de l'Univ. Pierre et Marie Curie **79** (1986), n^o 4.

[6] N. Koblitz, *p-adic analysis: a short course on recent work*, London Mathematical Society Lecture Note Series **46**, Cambridge University Press, Cambridge (1980).

[7] Ch. Pisot, *Sur les fonctions analytiques arithmétiques et presque arithmétiques*, C. R. Acad. Sci. Paris **222** (1946), 1027–1028.

[8] G. Pólya, *Über ganzwertige ganze Funktionen*, Rend. Circ. Math. Palermo **40** (1915), 1–16.

[9] P. Stäckel, *Über arithmetische Eigenschaften analytischer Functionen*, Math. Annalen **46** (1895), 513–520.

Some Geometry of Numbers for Function Fields

Jeff Thunder
(joint work with Chris Hurlburt)

Classically, Hermite's constant is defined as follows. For a positive integer $n > 1$, γ_n is the smallest number such that, for every positive definite quadratic form $F(\mathbf{X}) \in \mathbb{R}[\mathbf{X}]$ in n variables, there is a non-zero integer point $\mathbf{z} \in \mathbb{Z}^n$ with

$$\frac{F(\mathbf{x})}{\operatorname{disc}(F)^{1/n}} \leq \gamma_n,$$

where $\operatorname{disc}(F)$ is the discriminant of F.

Hermite's constant can also be defined in terms of lattices and geometry of numbers. Specifically,

$$\gamma_n = \sup_{\Lambda} \frac{\lambda_1(\Lambda)2}{\det(\Lambda)^{2/n}},$$

where the supremum is over lattices $\Lambda \subset \mathbb{R}^n$ of rank n, $\lambda_1(\Lambda)$ denotes the first successive minimum of Λ with respect to the unit ball, and $\det(\Lambda)$ denotes the determinant of Λ. With this in mind, it is not difficult to state the definition of Hermite's constant in terms of twisted heights:

$$\gamma_n = \sup_{A} \inf_{\xi} \frac{H_A(\xi)2}{|\det(A)|^{2/n}},$$

where the supremum is over $A \in \mathrm{GL}_n(\mathbb{Q}_{\mathbb{A}})$ (the general linear group over the adeles of $\mathbb{Q}$), the infimum is over ξ in projective $(n-1)$-space over $\mathbb{Q}$, and $|\det(A)|$ is the adelic modulus. From this, one is lead to a "Hermite's constant" over any field with a product formula - including function fields.

Let K be a finite algebraic extension of the field of rational functions $\mathbb{F}_q(X)$, where X is transcendental over the field with q elements, $\mathbb{F}_q$. We assume that $\mathbb{F}_q$ is the field of constants for K. Let g and J denote the genus and the number of divisor classes of degree 0, respectively (J is also the cardinality of the Jacobian). Let ζ_K denote the zeta function of K which is analogous to the classical Riemann zeta function and let $K_{\mathbb{A}}$ denote the adele ring. For $A \in \mathrm{GL}_n(K_{\mathbb{A}})$, let h_A denote the (additive) twisted height. For $A \in \mathrm{GL}_n(K_{\mathbb{A}})$, set $\lambda_1(A)$ to be the minimum over all $\xi \in \mathbb{P}^{n-1}(K)$ of $h_A(\xi)$. We then have an analog of Hermite's constant:

$$\gamma_n(K) := \sup_{A \in \mathrm{GL}_n(K_{\mathbb{A}})} \lambda_1(A) + (1/n) \deg \operatorname{div} \det(A).$$

The analog of Minkowski's theorem gives $\gamma_n(K) \leq g$ for all $n > 1$. We make the conjecture that $\gamma_n(K) = g$ for all $n > 1$. The case $A = I_n$ shows that the conjecture is true when $g = 0$. We prove the conjecture in many cases.

Theorem 2. *If $g = 1$, then $\gamma_2(K) = 1$.*

The proof of this is via an explicit construction. We can prove more via some measure theory. Let G_n denote the subgroup of $\mathrm{GL}_n(K_{\mathbb{A}})$ consisting of those A with $\deg \operatorname{div} \det(A) = 0$, and for notational convenience set $\Gamma_n = \mathrm{GL}_n(K)$. We construct a haar measure on μ_n on G_n normalized so that $\mu_n(G_n/\Gamma_n) = 1$. Let H_n be the subgroup of G_n consisting of those A where $\operatorname{div} \det(A)$ is linearly equivalent to the zero divisor.

Theorem 3. *Suppose $n_K \in \mathbb{N}$ satisfies $q^{n_K}(q-1)(1-q^{-n_K}) \geq J$. Then for all $n > n_K$, all m with $-n < m \leq -n_K$ and all $A \in \mathrm{GL}_n(K_{\mathbb{A}})$ with $\deg \operatorname{div} \det(A) = m$ there is a set of $B\Gamma_n \in G_n/\Gamma_n$ of positive measure with with $\lambda_1(AB) = g$. In particular, $\gamma_n(K) = g$ for all $n \geq n_K$.*

Theorem 4. *Suppose $g = 1$. If J is even, then for some $A \in G_2$ there is a set of $B\Gamma_2 \in H_2/\Gamma_2$ of positive measure with $\lambda_1(AB) = 1$.*

Theorem 5. *Suppose $g = 1$, $q > 2$ and J is odd. Then with the exception of the cases $q = 3, J = 7$ and $q = 4, J = 9$, for every $A \in G_2$ there is a set of $B\Gamma_2 \in H_2/\Gamma_2$ of positive measure with $\lambda_1(AB) = 1$.*

The number of exceptions to Roth's theorem

Wolfgang Schmidt

A general version of Roth's theorem is as follows. Let K be a number field, S a finite, non-empty set of places of K, and for each $v \in S$, let $\|\cdot\|_v$ be a suitably normalized absolute value belonging to v, and $\xi_v \in K_v$ algebraic over K, where K_v is the completion of K with respect to $\|\cdot\|_v$. Also let μ_v for $v \in S$ be nonnegative reals with $\sum_{v\in S} \mu_v = 2 + \delta$, where $0 < \delta < 1$. Then the system of inequalities

$$\|\xi_v - \alpha\|_v < H(\alpha)^{-\mu_v} \qquad (v \in S), \tag{1}$$

where $H(\alpha)$ is the absolute height of α, has only finitely many solutions in $\alpha \in K$.

We are interested in the number of "exceptions" to Roth's theorem, i.e. the number of $\alpha \in K$ satisfying (1). Bounds for the number "large" solutions, i.e. solutions with $H(\alpha) > e^{3/\delta}$, can be given by well established methods, e.g.

$$\ll \frac{\log^+ \log^+ H_0}{\log(1+\delta)} + \delta^{-1} \log(2s^2 D) \log\log(2s^2 D),$$

where $s = |S|$, $H(\xi_v) \leq H_0$ and $[K(\xi_v) : K] \leq D$ for $v \in S$.

Now we give the estimate

$$\delta^{-1}(2\sqrt{3})^d \log^+(d/\delta)$$

for the number of "small" solutions, i.e. solutions satisfying $H(\alpha) \leq e^{3/\delta}$. Here $d = \deg K$ and the δ in the logarithm can be omitted when S contains an archimedean place. In fact this holds whether the numbers ξ_v are algebraic or not. The constants in $\ll$ are absolute.

Dimension estimates for vector spaces generated by values of certain q-series

Peter Bundschuh

Here we consider the entire transcendental functions

$$f_0(z) := \prod_{j=0}^{\infty} P(zq^{-jm}) \quad \text{and} \quad f_h(z) := \sum_{i=0}^{\infty} q^{-him} \prod_{j=0}^{i-1} P(zq^{-jm}) \quad (h = 1, 2, ...),$$

where the assumptions on P, q, m will be stated in a moment. These functions satisfy the Poincaré functional equation

$$f(q^m z) = aP(q^m z)f(z) + b \qquad \text{with } a := q^{-hm},\ b := 1 - \delta_{h,0}, \tag{1}$$

δ the Kronecker symbol. Our principal result on these functions is the following.

Main Theorem. *Let K be either $\mathbb{Q}$ or an imaginary quadratic number field, let $q \in O_K$, the ring of integers in K, satisfy $|q| > 1$, and let $m \in \mathbb{N}$. Suppose $P \in K[X], P(0) = 1, \deg P =: \ell \in \mathbb{N}$ and $P(q^{-k}) \neq 0$ for any $k \in \mathbb{N}_0 := \mathbb{N} \cup \{0\}$. Then, denoting*

$$\Delta := \dim_K K + \sum_{\mu=0}^{m-1} K f_h(q^{-\mu}),$$

we have the lower bounds

$$\Delta \geq \frac{(m+1)^2 - \ell m}{\ell(m+2)} \quad \text{if } m \geq 2\ell, \quad \Delta \geq \frac{(m+1)^2 + \ell(m+2)}{\ell(\ell m + m + 2)} \quad \text{if } m \geq \ell^2 - 2 \tag{2}$$

uniformly in $h \in \mathbb{N}_0$.

We remark that $P(q^{-k}) = 0$ for some $k \in \mathbb{N}_0$ would imply $f_h(q^{-\mu}) \in K$ for $\mu \in \{0, ..., m-1\}$ with $\mu \equiv k \pmod m$. We further notice that all $f_h(q^{-\mu})$ can be expressed as values of basic hypergeometric series with suitable parameters at appropriate points.

Since the lower bounds for Δ in (2) are greater than 1 if and only if $m \geq 2\ell, m \geq \ell^2 - 2$, respectively, we have the following immediate consequence of our Main Theorem.

Theorem 1. *Assume the hypotheses of the Main Theorem, and let $h \in \mathbb{N}_0$. If $m \geq \min(2\ell, \ell^2 - 2)$ then at least one of the numbers $f_h(q^{-\mu}), \mu = 0, ..., m-1$, is not in K.*

We remark that the case $\ell = 1, m = 1, h = 0$ was first settled by Lototsky [7], whereas we solved essentially the case $\ell = 2, m = 2, h = 0$ in [3] after work of Zhou and Lubinsky [13], who assumed $K = \mathbb{Q}, q > 1, P \in \mathbb{Q}_+[X]$. Under the same restrictive hypotheses, Zhou [12] treated the case $\ell = 2, m \geq 2, h = 1$ separately.

It should be also remarked that we proved very recently in [4] the above Theorem 1 for $h = 0$ and $h = 1$ under the much stronger condition $m \geq \max(\ell, \ell(\ell - 1))$ using our old irrationality criterion in [2], which is based on Newton interpolation

series. Notice that $\min(2\ell, \ell^2-2)$ is essentially linear in ℓ, whereas $\max(\ell, \ell(\ell-1))$ is quadratic.

Comparing both lower bounds for Δ in (2), we recognize that the first is not smaller than the second if and only if $\ell \le m-(5m+4)/m^2$ holds. Hence we have the first assertion in

THEOREM 2. *Assume the hypotheses of the Main Theorem and $h \in \mathbb{N}_0$. Then*

$$\Delta \ge \frac{(m+1)^2-\ell m}{\ell(m+2)}, \tag{3}$$

holds if $\ell \ge 2$ and $m \ge 2\ell$. If $\ell = 2$ and $m \in \{2,3\}$ then we have $\Delta \ge 2$. Inequality (3) holds also for $\ell = 1, m \ge 4$. But if $\ell = 1, m \in \{1,2,3\}$ we have $\Delta \ge (m^2+3m+3)/(2m+2)$ implying $\Delta = m+1$ for $m \in \{1,2\}$.

Notice that from (3) we can never deduce $\Delta = m+1$. Namely this would be possible exactly if the right-hand side in (3) is strictly larger than m, and this is equivalent with $\ell < (m+1)^2/(m^2+3m)$ (≤ 1). The two cases $(\ell, m) = (1,1)$ and $(1,2)$ are the only ones, where we can deduce linear independence results from our Main Theorem. We still can conclude $\Delta \ge m$ for any $m \in \mathbb{N}$ and $h \in \mathbb{N}_0$ if we suppose $\ell = 1$. But note that in this case $\ell = 1, \Delta = m+1$ for any $m \in \mathbb{N}$ is known for $h = 0$, compare Bézivin [1] for an ineffective version, and Väänänen [11] for an effective one.

In the cases of arbitrary $h \in \mathbb{N}_0$ and $(\ell, m) = (1,1)$ or $(1,2)$, we are able to write down the following quantitative versions, both under the hypotheses of the Main Theorem.

THEOREM 3. *For every $(u, v) \in O_K^2$ with $|v| > 1$, we have*

$$|u + v f_h(1)| > |v|^{-(4/3)-\varepsilon_1(|v|)}.$$

THEOREM 4. *For every $(u, v_1, v_2) \in O_K^3$ with $v := \max(|v_1|, |v_2|) > 1$ we have*

$$|u + v_1 f_h(1) + v_2 f_h(q^{-1})| > v^{-12-\varepsilon_2(v)}.$$

In these two theorems, the $\varepsilon_j(x)$ appearing in the exponents are of the shape $\gamma(\log x)^{-1/2}$ with $\gamma > 0$ independent of u and the v's. Remark that Theorem 3 was first proved for $h = 0$ by the present author [2] and later by Popow [9].

The basic ingredient of the *proof of the Main Theorem* is Nesterenko's dimension estimate [8], more precisely, its generalizations to fields of type K. To apply this tool, one has to construct an infinite sequence of linear forms in $1, f_h(1), \ldots, f_h(q^{-(m-1)})$ (indexed by N, say), whose absolute values tend sufficiently rapidly to zero as $N \to \infty$, whereas the maximum of the absolute values of their coefficients do not increase with N too quickly. To construct such a sequence, we use the

integrals

$$I_{\pm}(N) := \frac{1}{2\pi i} \oint\limits_{\Gamma_{\pm}(N)} \frac{f_h(z)dz}{z^N \prod_{j=0}^{M}(z - q^{\pm j})} \tag{4}$$

with appropriately chosen (large) $M = M(N)$ and suitable circles $\Gamma_{\pm}(N)$ around the origin. By a very careful analysis, the asymptotic relation $|I_{\pm}(N)| \sim |c_{h,N+M}|$ can be established for $N \to \infty, c_{h,k}$ being the Taylor coefficients of f_h about the origin. For this asymptotic equality and for the evaluation of $|c_{h,N+M}|$ in terms of N, one profits by the fact that the analytic growth of the solutions of (1) and of their Taylor coefficients were studied in the past in very much detail.

In the arithmetic part of the proof, one evaluates $I_{\pm}(N)$ from (4) and expresses the arising $f_h(q^{\pm j})$ by the m numbers $f_h(q^{-\mu})$ via iteration of (1). Thus, one is lead to linear forms in 1 and $f_h(q^{-\mu}), \mu = 0, ..., m-1$, with explicit coefficients in K. These have to be transformed into O_K-linear forms by multiplication by some appropriate $\Omega_{\pm}(N) \in O_K \setminus \{0\}$, whose growth with N has to be precisely controlled, and is different in the $+$ and $-$ case, altogether giving rise to the two cases in (2).

To prove Theorems 3 and 4, we use just the linear forms over O_K constructed before. But to conclude, we apply our quantitative refinements with Töpfer [6],[10] of the Nesterenko type criterion. Full proofs can be found in [5].

References

[1] J.-P. Bézivin, *Indépendance linéaire des valeurs des solutions transcendantes de certaines équations fonctionnelles*, Manuscripta Math. **61** (1988), 103-129.

[2] P. Bundschuh, *Ein Satz über ganze Funktionen und Irrationalitätsaussagen*, Invent. Math. **9** (1970), 175-184.

[3] P. Bundschuh, *Again on the irrationality of a certain infinite product*, Analysis **19** (1999), 93-101.

[4] P. Bundschuh, *Note on the irrationality of certain multivariate q-functions*, Taiwanese J. Math. **10** (2006), 603-611.

[5] P. Bundschuh, *Arithmetical results on certain q-series*, Internat. J. Number Theory (to appear).

[6] P. Bundschuh and T. *Töpfer, Über lineare Unabhängigkeit*, Mh. Math. **117** (1994), 17-32.

[7] A.V. Lototsky, *Sur l'irrationalité d'un produit infini*, Mat. Sb. **12 (54)** (1943), 262-271.

[8] Yu.V. Nesterenko, *On the linear independence of numbers (in Russian)*, Vestn. Mosk. Univ., Ser. I, **40** (1985), 46-49; Engl.transl.: *Mosc. Univ. Math. Bull.* **40** (1985), 69-74.

[9] A.Yu. Popov, *Arithmetical properties of values of some infinite products (in Russian)*, in Diophantine Approximations, Part II, pp. 63-78, Moskov. Gos. Univ., Moscow, 1986.

[10] T. Töpfer, *Über lineare Unabhängigkeit in algebraischen Zahlkörpern*, Result. Math. **25** (1994), 139-152.

[11] K. Väänänen, *On linear independence of the values of generalized Heine series*, Math. Ann. **325** (2003), 123-136.

[12] P. Zhou, *On the irrationality of a certain series of two variables*, in Approximation Theory XI, pp. 439-451. Modern Methods Math., Nashboro Press, Brentwood, TN, 2005.

[13] P. Zhou and D.S. Lubinsky, *On the irrationality of* $\prod_{j=0}^{\infty}(1 \pm q^{-j}r + q^{-2j}s)$, Analysis **17** (1997), 129-153.

Reporter: Victor Beresnevich

Participants

Prof. Dr. Boris Adamczewski
Institut Camille Jordan
UFR de Mathematiques
Univ. Lyon 1; Bat. Braconnier
21, Avenue Claude Bernard
F-69622 Villeurbanne Cedex

Prof. Dr. Michael Bennett
Dept. of Mathematics
University of British Columbia
1984 Mathematics Road
Vancouver , BC V6T 1Z2
CANADA

Prof. Dr. Victor Beresnevich
Dept. of Mathematics
University of York
GB-Heslington, York Y010 5DD

Prof. Dr. Vasilii Bernik
Fakultät für Mathematik
Universität Bielefeld
33501 Bielefeld

Prof. Dr. Yuri Bilu
Mathematiques et Informatique
Universite Bordeaux I
351, cours de la Liberation
F-33405 Talence Cedex

Prof. Dr. W.Dale Brownawell
Department of Mathematics
Pennsylvania State University
University Park , PA 16802
USA

Prof. Dr. Yann Bugeaud
Institut de Mathematiques
Universite Louis Pasteur
7, rue Rene Descartes
F-67084 Strasbourg Cedex

Prof. Dr. Peter Bundschuh
Mathematisches Institut
Universität zu Köln
Weyertal 86 - 90
50931 Köln

Prof. Dr. Pietro Corvaja
Dipartimento di Matematica e
Informatica
Universita di Udine
Via delle Scienze 206
I-33100 Udine

Emmanuel Delsinne
Laboratoire LMNO
CNRS UMR 6139
Universite de Caen
BP 5186
F-14032 Caen -Cedex

Prof. Dr. Andrej Dujella
Department of Mathematics
University of Zagreb
Bijenicka 30
10000 Zagreb
CROATIA

Dr. Jan-Hendrik Evertse
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Prof. Dr. Clemens Fuchs
Departement Mathematik
ETH-Zentrum
Rämistr. 101
CH-8092 Zürich

Aurelien Galateau
Theorie des Nombres
Institut de Math. de Jussieu
Universite Paris 6
4, Place Jussieu
F-75005 Paris

Prof. Dr. Kalman Györy
Institute of Mathematics
University of Debrecen
Pf. 12
H-4010 Debrecen

Philipp Habegger
Mathematisches Institut
Universität Basel
Rheinsprung 21
CH-4051 Basel

Prof. Dr. Noriko Hirata-Kohno
College of Science and Technology
Nihon University
1-8,Suraga-dai, Kanda
Tokyo 101-8308
JAPAN

Prof. Dr. Christian Krattenthaler
Institut für Mathematik
Universität Wien
Nordbergstr. 15
A-1090 Wien

Prof. Dr. Michel Laurent
Institut de Mathematiques
de Luminy
Case 907
163 Avenue de Luminy
F-13288 Marseille Cedex 9

Prof. Dr. David W. Masser
Mathematisches Institut
Universität Basel
Rheinsprung 21
CH-4051 Basel

Prof. Dr. Yuri Matiyasevich
St. Petersburg Branch of
Mathematical Institute of
Russian Academy of Science
Fontanka 27
191023 St. Petersburg
RUSSIA

Guillaume Maurin
Institut Fourier
UMR 5582; CNRS/UJF
Universite de Grenoble I
100 rue de Maths
F-38402 Saint-Martin d'Heres

Prof. Dr. Preda Mihailescu
Mathematisches Institut
Georg-August-Universität
Bunsenstr. 3-5
37073 Göttingen

Prof. Dr. Yuri V. Nesterenko
Dept. of Mechanics and Mathematics
Moscow Lomonosov State University
Vorobjovy Gory
119899 Moscow
RUSSIA

Prof. Dr. Patrice Philippon
Equipe "Geometrie et dynamique"
Institut Mathematique de Jussieu
175 rue du Chevaleret
F-75013 Paris

Gabriele Ranieri
Dip. di Matematica "L.Tonelli"
Universita di Pisa
Largo Bruno Pontecorvo,5
I-56127 Pisa

Dr. Nicolas Ratazzi
Laboratoire de Mathematiques
Universite Paris Sud (Paris XI)
Batiment 425
F-91405 Orsay Cedex

Prof. Dr. Gael Remond
Institut Fourier
UMR 5582; CNRS/UJF
Universite de Grenoble I
100 rue de Maths
F-38402 Saint-Martin d'Heres

Prof. Dr. Tanguy Rivoal
Institut Fourier
UMR 5582; CNRS/UJF
Universite de Grenoble I
100 rue de Maths
F-38402 Saint-Martin d'Heres

Prof. Dr. Damien Roy
Department of Mathematics
University of Ottawa
Ottawa , Ont. K1N 6N5
CANADA

Prof. Dr. Andrzej Schinzel
Institute of Mathematics of the
Polish Academy of Sciences
P.O. Box 21
ul. Sniadeckich 8
00-956 Warszawa
POLAND

Prof. Dr. Hans Peter Schlickewei
Fachbereich Mathematik
Universität Marburg
Hans-Meerwein-Str.
35043 Marburg

Prof. Dr. Wolfgang M. Schmidt
Dept. of Mathematics
University of Colorado
Campus Box 395
Boulder , CO 80309-0395
USA

Prof. Dr. Cameron L. Stewart
Dept. of Pure Mathematics
University of Waterloo
200 University Avenue West
Waterloo , Ont. N2L 3G1
CANADA

Prof. Dr. Jeff L. Thunder
Dept. of Mathematics
Northern Illinois University
DeKalb , IL 60115
USA

Prof. Dr. Robert F. Tichy
Institut für Mathematik
Technische Universität Graz
Steyrergasse 30
A-8010 Graz

Prof. Dr. Jeffrey D. Vaaler
Department of Mathematics
University of Texas at Austin
1 University Station C1200
Austin , TX 78712-1082
USA

Prof. Dr. Eric Villani
Department of Mathematics
University of Ottawa
Ottawa , Ont. K1N 6N5
CANADA

Prof. Dr. Carlo Viola
Universita di Pisa
Dipartimento di Matematica
Via Buonarroti
I-56127 Pisa

Prof. Dr. Michel Waldschmidt
Institut de Mathematiques
175, rue du Chevaleret
F-75013 Paris

Martin Widmer
Mathematisches Institut
Universität Basel
Rheinsprung 21
CH-4051 Basel

Prof. Dr. Wadim Zudilin
V.A. Steklov Institute of
Mathematics
Russian Academy of Sciences
8, Gubkina St.
119991 Moscow GSP-1
RUSSIA