Mathematisches Forschungsinstitut Oberwolfach

Report No. 22/2012

DOI: 10.4171/OWR/2012/22

Diophantische Approximationen

Organised by
Yann Bugeaud, Strasbourg
Yuri V. Nesterenko, Moscow

April 22nd – April 28th, 2012

Abstract. This Number Theoretic conference was focused on the following subjects: the Littlewood conjecture, simultaneous homogeneous and inhomogeneous Diophantine approximation, geometry of numbers, irrationality, Diophantine approximation in function fields, counting questions in number fields, effective methods for resolution of Diophantine equations

Mathematics Subject Classification (2000): 11-06.

Introduction by the Organisers

The workshop *Diophantische Approximationen* (Diophantine approximations), organised by Yann Bugeaud (Strasbourg) and Yuri V. Nesterenko (Moscow) was held April 22nd – April 28th, 2012. There have been 26 participants with broad geographic representation. This workshop gathered researchers with various backgrounds. Below we briefly recall the topics discussed, thus outlining some of the modern lines of investigation in Diophantine approximation. We refer the reader to the abstracts for more details.

Loosely speaking Diophantine approximation is a branch of Number Theory that can be described as the 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 rational approximation to irrational numbers. A celebrated open problem in this direction is the Littlewood conjecture, which asserts that, for every real numbers α, β and every positive ε, there exists a positive integer q such that

$$q \cdot \|q\alpha\| \cdot \|q\beta\| < \varepsilon.$$

Here, $\| \cdot \|$ denotes the distance to the nearest integer. Talks of Badziahin and Harrap were concerned with this problem and some of its variants. Also, Roy, Moshchevitin, Laurent, Beresnevich and German have presented new results on simultaneous homogeneous and inhomogeneous Diophantine approximation.

Another topic of current interest in Diophantine approximation are irrationality and transcendence statements. Major open questions include the status of the Riemann zeta function evaluated at odd integers and of the values of polylogarithms. New advances on these and related problems were presented by Viola, Marcovecchio, Zudilin and Hirata-Kohno.

Diophantine approximation in function fields was presented by Corvaja (estimates for greatest common divisors) and Adamczewski (diagonal of algebraic power series).

Various questions on number fields have been discussed by Widmer (counting algebraic numbers with bounded height and degree), Stewart (counting exceptional units) and Habegger (Northcott's property). Amoroso considered overdetermined systems of lacunary equations from an algorithmic point of view.

Diophantine equations remain a subject of constant interest. Fuchs considered equations of the form $f(x) = g(y)$. Evertse presented new effective upper bounds for the size of solutions to classical Diophantine equations over finitely generated domains. Kovács was interested in fifth powers and almost fifth powers in arithmetic progressions, a problem motivated by a celebrated result of Erdős and Selfridge. Bennett explained how a variety of techniques ranging from Diophantine approximation to modular methods allows one to solve certain families of equations of the form $f(x, y) = z^p$ in all four variables, where $f(x, y)$ is an homogeneous integer polynomial of degree $3, 4, 6$ or 12.

Workshop: Diophantische Approximationen

Table of Contents

Abstracts

Separated-variables equations and related questions

Clemens Fuchs

In various contexts equations of separated-variables type turn out to be relatively easy to solve and thus it is reasonable to expect that one can say more than in the general case also from the Diophantine point of view, i.e. when looking at $f(x) - g(y) = 0, f, g \in \mathbb{Z}[X]$, with $x, y \in \mathbb{Z}$. Examples for equations of this type include integral points on elliptic, hyper- and superelliptic equations, but also equations of the form $\binom{x}{a} = y^b$ for given integers $a > 1, b > 1$, etc. Observe that the decidability of the finiteness of the number of solutions was solved by Siegel in his famous paper.

It is well-known that one has the following explicit criterion to check if a given equation of separated-variables type has finitely many solutions or not; this statement is known as the [Bilu - Tichy] *criterion*: Let $f, g \in \mathbb{Q}[X]\backslash\mathbb{Q}$. The following statements are equivalent:

- $f(x) = g(y)$ has infinitely many integral solutions.
- $\exists\varphi \in \mathbb{Q}[X], \lambda, \mu \in \mathbb{Q}[X]$ linear, $f_1, g_1 \in \mathbb{Q}[X]$ s.t.
  1. $f = \varphi \circ f_1 \circ \lambda, g = \varphi \circ g_1 \circ \mu$,
  2. $f_1(x) = g_1(y)$ has infinitely many integral solutions,
  3. (f_1, g_1) or (g_1, f_1) is one of the following

Type	Explicit form of (f, g)
1.	$(X^q, \alpha X^r v(X)^q)$
2.	$(X^2, (\alpha X^2 + \beta)v(X)^2)$
3.	$(D_s(X, \alpha^t), D_t(X, \alpha^s))$
4.	$(\alpha^{-s/2} D_s(X, \alpha), -\beta^{-t/2} D_t(X, \beta))$
5.	$((\alpha X^2 - 1)^3, 3X^4 - 4X^3)$

where $D_n(X + \alpha/X, \alpha) = X^n + (\alpha/X)^n$ are the Dickson polynomials. In these cases we indeed have infinitely many solutions.

(Very rough) Sketch of the proof: "$\Leftarrow$": trivial; "$\Rightarrow$": $\exists E(x, y) | f(x) - g(y)$ irreducible s.t. $E(x, y) = 0$ has infinitely many solutions $\Rightarrow E$ is necessarily absolutely irreducible. By Siegel's theorem it follows that $E(x, y) = 0$ defines a curve with genus 0 and at most two points at infinity. By Fried: $f = f_1 \circ f_2, g = g_1 \circ g_2$, $\deg f_1 = \deg g_1$ and $\exists e$ absolutely irreducible s.t. $e(x, y)|f_1(x) - g_1(y)$ and $E(x, y) = e(f_2(x), g_2(y))$. It follows that $\deg e \leq 2$ and hence by Bilu $f_1 = \varphi_1 \circ f_3$, $g_1 = \varphi_1 \circ g_3$ and either $e(x, y) = f_3(x) - g_3(y)$, which then is done by Ritt's 2nd theorem, or $e(x, y)|f_3(x) - g_3(y)$ and $f_3(x) = D_n(x + b, a), g_3(y) = -D_n((cx + d)\cos(2\pi/n), a)$, which then is done by direct arguments. //

Observe that [Fried]'s input to the proof brings a crucial new idea and that it is geometric in nature; it says that one should look at the curve $f(x) - g(y) = 0$ as given by the fiber product of the two covers of $\mathbb{P}^1$ defined by $f(x) - z = 0$ and

$g(y) - z = 0$, respectively. In this way one turns the problem into questions in combinatorics and group theory.

We turn to the following question: *Is it true that all but finitely many of the solutions satisfy* $f_1(\lambda(x)) = g_1(\mu(y))$*?* In general the answer is no! However, we have:

Theorem ([Bilu - F. - Luca - Pinter]**).** *Yes, unless*

1. (f_1, g_1) *is of type* 1 *or* 3*,* $\varphi(X) = \varphi(-X)$ *and almost all solutions satisfy* $f_1(\lambda(x)) = \pm g_1(\mu(y))$.
2. (f_1, g_1) *is of type* 1*,* $\varphi(X) = \varphi(a - X)$ *for some* $a \in \mathbb{Q}^*$ *and all but finitely many solutions satisfy* $f_1(\lambda(x)) = g_1(\mu(y))$ *or* $f_1(\lambda(x)) + g_1(\mu(y)) = a$*. Moreover,* n *is odd and* $(f_1, g_1) = (X^2, (a/4)D_n(X - 2, 1) + (a/2))$.

Sketch of the proof: Use Siegel's theorem to prove that almost all solutions of $\varphi(x) = \varphi(y)$ satisfy $x = y$ or $x + y = a$ (then $\varphi(X) = \varphi(a - X)$). Then use Fried's genus formula and Siegel's theorem to prove that

$$f_1(x) + g_1(y) = a$$

with (f_1, g_1) a standard pair s.t. $f_1(x) = g_1(y)$ has infinitely many solutions (and $a \neq 0, \deg f_1, \deg g_1 \geq 3$ if (f_1, g_1) is of 1. or 3. kind) has only finitely many solutions. Finally consider cases and use properties of Dickson-polynomials. //

This additional information to the Bilu-Tichy criterion turns out to be useful in applications when one has to exclude standard pairs. In [Bilu - F. - Luca - Pinter] we have applied it to show that certain combinatorial Diophantine equation involving Stirling numbers have only finitely many solutions in integers.

Another question that arises when applying the Bilu-Tichy criterion is the following: *Is there a method (i.e. an algorithm) to find for a given polynomial* f *all decompositions? More generally: Is it possible to describe all composite* f*'s and all their decompositions algorithmically?*

Here an example to see what one can expect: Given $f = X^6 + a_1X^5 + a_2X^4 + a_3X^3 + a_4X^2 + a_5X + a_6 \in \mathbb{C}[a_1, \dots, a_6][X]$ with $f = g \circ h$. Clearly, the degree d of h is a divisor of 6. Let e.g. $d = 3$. We need g, Q, R with $f = g \circ Q + R$ s.t. $\deg(f - Q^2) < \deg f/2 = 3$ (such g, Q, R always exist and there is a unique choice). To get a decomposition we must have $R = 0$ and then all decompositions with $h = Q$ are of degree 3! Ansatz for $Q = X^3 + b_1X^2 + b_2X + b_3 \in \mathbb{C}[b_1, b_2, b_3][X]$. The condition on the degree gives $2b_1 = a_1, 2b_2 = a_2 - b_1^2, 2b_3 = a_3 - 2b_1b_2$. Thus $R = (a_4 - 2b_1b_3 - b_2^2)X^2 + (a_5 - 2b_2b_3)X, g = X^2 + a_6 - b_3^2$. $R = 0$ gives $a_4 - 2b_1b_3 - b_2^2 = 0, a_5 - 2b_2b_3 = 0$. In summary we have (this is a reformulation of a result of [Bodin]): Given n. There exist (everything effectively computable) $J \in \mathbb{N}$ and for all $1 \leq j \leq J$: $\mathcal{V}_j \subseteq \mathbb{A}^{t_j + n/t_j}/\mathbb{Q}$ with $t_j | n$ and $F_j, G_j, H_j \in \mathbb{Q}[\mathcal{V}_j][X]$ with $F_j = G_j \circ H_j$ and $\deg F_j = n$ s.t.: If $f = g \circ h \in \mathbb{C}[X]$ with $\deg f = n$, then there is a j and $P \in \mathcal{V}_j(\mathbb{C})$ with $g(X) = G_j(P, X), h(X) = H_j(P, X)$, and $f(x) = F_j(P, X)$.

The question arises if more is true, e.g. an analogue to polynomials that are lacunary in the sense that its number of terms is fixed. A positive answer along the above lines was given by [Zannier]. So does the same hold for rational functions? A first result in this direction is the following:

Theorem ([F. - Zannier]). *Given ℓ and $f(X) = g(h(X)) = P(X)/Q(X)$ with $g, h \in \mathbb{C}(X)$, $P, Q \in \mathbb{C}[X]$ not necessarily coprime and having ℓ terms. If $h(X) \neq \lambda(aX^n + bX^{-n}), \lambda \in \mathrm{PGL}_2(\mathbb{C}), a, b \in \mathbb{C}$, $n \in \mathbb{N}$, then* $\deg g \leq 2016 \cdot 5^{\ell}$.

Sketch of the proof: We take a "suitable" conjugate $y \neq x$ of x over $\mathbb{C}(h)$, i.e. $h(x) = h(y)$. Since $f = g(h) \in \mathbb{C}(h)$, we have $f(x) = f(y)$. It follows $P(x)Q(y) - P(y)Q(x) = 0$. This is a S-unit equation over $K = \mathbb{C}(x, y)$ with "few" terms. After normalizing we get for $z = x^m y^n$:

$$\frac{2\delta \deg f}{63 \cdot 3^{\ell}} \leq [K : \mathbb{C}(z)] \leq \binom{\ell^2 - 1}{2}(|S| + 2g_K - 2) \leq 2\binom{\ell^2 - 1}{2}\delta^2$$

with $\delta = [K : \mathbb{C}(x)]$; the lower bound follows by the "suitability" of y (the existence is proved by using the theory of function fields, Puiseux-expansion, group and Galois-theory). It follows $\deg f = \deg g \deg h \ll_{\ell} \deg h$ and thus $\deg g \ll_{\ell} 1$.//

The last theorem says that if $f = g \circ h$ with $\deg g$ large and h not "special", then f necessarily has many terms; it is a first step toward a classification that we expect also to hold for composite rational functions.

References

[Bilu - Tichy] Y.F. Bilu and R.F. Tichy, *The Diophantine equation $f(x) = g(y)$*, Acta Arith. **95** (2000), 261-288.

[Bilu - F. - Luca - Pinter] Y.F. Bilu, C. Fuchs, F. Luca, and A. Pinter, *Combinatorial Diophantine equations and a refinement of a theorem on separated varibles equations*, Publ. Math. Debrecen, to appear.

[Bodin] A. Bodin, *Decomposition of polynomials and approximate roots*, Proc. Amer. Math. Soc. **138** (2010), 1989-1994.

[F. - Zannier] C. Fuchs and U. Zannier, *Composite rational functions expressible with few terms*, J. Eur. Math. Soc. (JEMS) **14** (2012), 175-208.

[Fried] M. Fried, *The field of definition of function fields and a problem on the reducibility of polynomials in two variables*, Illinois J. Math. **17** (1973), 128-146.

[Zannier] U. Zannier, *On composite lacunary polynomials and a conjecture of Schinzel*, Invent. Math. **174** (2008), 127-138.

On the coefficients of linear forms in polylogarithms

Carlo Viola

If an n-dimensional integral ($n \geq 1$) of a rational function over the product of n paths having distinct endpoints in $\mathbb{C}$ represents a linear form in zeta-values or in polylogarithms, then the n-fold contour integral of the same rational function around the poles yields the leading coefficient of the linear form. Several special instances of this principle are known, though we miss a general proof of it. We quote e.g. the following, partially proved in [4], Theorem 3.1:

For any $n \geq 2$ and any non-negative integers $h_1, \ldots, h_n; j_1, \ldots, j_n; k$ such that $h_r + k - h_1 \geq 0$ $(r = 2, \ldots, n-1)$ we have

$$\int_0^1 \cdots \int_0^1 \frac{x_1^{h_1}(1-x_1)^{j_1} \cdots x_n^{h_n}(1-x_n)^{j_n}}{\big(1-(1-x_1\cdots x_{n-1})x_n\big)^{j_n+h_1-k+1}} \,\mathrm{d}x_1 \cdots \mathrm{d}x_n = a_1 + a_2\zeta(2) + \cdots + a_{n-1}\zeta(n-1) + a_n(n-1)\zeta(n), \tag{1}$$

where $a_1, a_2, \ldots, a_{n-1} \in \mathbb{Q}$ with controlled denominators and $a_n \in \mathbb{Z}$ (if $n \geq 3$ and $h_n + j_n \leq j_1 + \cdots + j_{n-1} + n - 3$ then $a_2 = 0$). Moreover the integer a_n has the following n-fold contour integral representation:

$$a_n = \frac{1}{(2\pi i)^n} \oint\limits_{|x_1|=\varrho_1} \cdots \oint\limits_{|x_{n-2}|=\varrho_{n-2}} \oint\limits_{\left|x_{n-1}-\frac{1}{x_1\cdots x_{n-2}}\right|=\varrho_{n-1}} \oint\limits_{\left|x_n-\frac{1}{1-x_1\cdots x_{n-1}}\right|=\varrho_n} \frac{x_1^{h_1}(1-x_1)^{j_1} \cdots x_n^{h_n}(1-x_n)^{j_n}}{\big(1-(1-x_1\cdots x_{n-1})x_n\big)^{j_n+h_1-k+1}} \,\mathrm{d}x_1 \cdots \mathrm{d}x_n \tag{2}$$

for any $\varrho_1, \ldots, \varrho_n > 0$.

In order to prove the irrationality of $\zeta(n)$, suitable $\mathbb{Q}$-linear combinations only of 1 and $\zeta(n)$ are required. Therefore it is desirable to have further information on the coefficients of $\zeta(2), \ldots, \zeta(n-1)$ in linear forms such as (1). A difficult and interesting problem is the search for integral representations of such intermediate coefficients. This appears to be related with some simultaneous Padé approximation problems to polylogarithms $\mathrm{Li}_j(1/t)$ for $t \to \infty$, and to powers of $\log t$ for $t \to 1$. In [1] Beukers proves the existence, for any $d \geq 0$, of polynomials $P(t)$, $Q(t)$ and $R(t)$ of degrees $\leq d$ such that

$$\begin{cases} P(t) + Q(t)\,\mathrm{Li}_1(1/t) + R(t)\,\mathrm{Li}_2(1/t) = O(t^{-d-1}) & (t \to \infty) \\ \qquad -Q(t) \qquad\qquad + R(t)\log t \quad = O\big((t-1)^{d+1}\big) & (t \to 1). \end{cases} \tag{3}$$

Beukers' result was extended in [2] by Fischler and Rivoal, who prove the existence, for any integers $n \geq 2$ and $d \geq 0$, of polynomials $P_0(t), P_1(t), \ldots, P_n(t) \in \mathbb{Q}[t]$ of degrees $\leq d$ satisfying

$$\begin{cases} P_0(t) + \displaystyle\sum_{j=1}^{n} P_j(t)\,\mathrm{Li}_j(1/t) = O(t^{-d-1}) & (t \to \infty) \\ \displaystyle\sum_{j=1}^{n} (-1)^{j-1} P_j(t)\,\frac{\log^{j-1} t}{(j-1)!} = O\big((t-1)^{(n-1)(d+1)}\big) & (t \to 1). \end{cases} \tag{4}$$

I recently found explicit integral representations for linear forms in polylogarithms $\mathrm{Li}_j(1/t)$, for polynomials in $\log t$ and for their coefficients, related to Padé-type approximation problems similar to the above. An example connected with

Beukers' problem (3) is the following, which can partially be found in [3], Theorem 2.1.

Let $t \in \mathbb{R}$, $t > 1$, and let $h, j, k, l, m \geq 0$ be integers. Define four double integrals (depending on h, j, k, l, m) as follows:

$$I_t^{(0,0)} = t^{-l-m} \int_0^1 \int_0^1 \frac{x^j(1-x)^h\, y^k(1-y)^l}{\big(x(1-y)+yt\big)^{j+k-m+1}}\,\mathrm{d}x\,\mathrm{d}y,$$

$$I_t^{(0,1)} = t^{-l-m} \int_0^1 \left(\frac{1}{2\pi i} \oint_{\left|y-\frac{x}{x-t}\right|=\varrho} \frac{x^j(1-x)^h\, y^k(1-y)^l}{\big(x(1-y)+yt\big)^{j+k-m+1}}\,\mathrm{d}y \right) \mathrm{d}x,$$

$$I_t^{(1,0)} = t^{-l-m} \frac{1}{2\pi i} \oint_{|x-t|=\sigma} \left(\int_0^1 \frac{x^j(1-x)^h\, y^k(1-y)^l}{\big(x(1-y)+yt\big)^{j+k-m+1}}\,\mathrm{d}y \right) \mathrm{d}x,$$

$$I_t^{(1,1)} = t^{-l-m} \frac{1}{2\pi i} \oint_{|x-t|=\sigma} \left(\frac{1}{2\pi i} \oint_{\left|y-\frac{x}{x-t}\right|=\varrho} \frac{x^j(1-x)^h\, y^k(1-y)^l}{\big(x(1-y)+yt\big)^{j+k-m+1}}\,\mathrm{d}y \right) \mathrm{d}x,$$

and let $\alpha = \max\{j+k,\, k+l,\, l+m\}$, $\beta = \max\{0,\, k+l-h\}$. With the above integrals one can associate the following linear polynomials in $\log t$:

$$I_t^{(0)} = I_t^{(0,0)} - I_t^{(0,1)} \log t, \qquad I_t^{(1)} = I_t^{(1,0)} - I_t^{(1,1)} \log t.$$

Then we have

$$t^\alpha (t-1)^\beta I_t^{(0)} = P(t) + R(t)\,\mathrm{Li}_2(1/t), \tag{5}$$

where $P(t), R(t) \in \mathbb{Q}[t]$ are polynomials with controlled degrees and denominators. Moreover

$$I_t^{(1,0)} = 0, \qquad R(t) = -t^\alpha (t-1)^\beta I_t^{(1,1)},$$

so that the leading coefficient $R(t)$ of the linear form (5) has the expected representation as a double contour integral. Also

$$\begin{cases} t^\alpha (t-1)^\beta I_t^{(0)} = P(t) + Q(t)\,\mathrm{Li}_1(1/t) + R(t)\,\mathrm{Li}_2(1/t) \\ t^\alpha (t-1)^\beta I_t^{(1)} = \qquad -Q(t) \qquad\qquad + R(t) \log t, \end{cases}$$

with $Q(t) = 0$, is a solution to a Padé-type approximation problem similar to (3). By estimating $I_t^{(0)}$ and $I_t^{(1,1)}$, and hence the linear form (5) and its leading coefficient $R(t)$, one gets the best known irrationality measures of $\mathrm{Li}_2(1/t)$ for rational t (see [3]).

The above construction can be extended to polylogarithms. For simplicity I state it for trilogarithms, with the following theorem.

Let $t \in \mathbb{R}$, $t > 1$, and let $h, j, k, l, m, p, q, r, s, w \geq 0$ be integers satisfying $j + s = m + r$. Similarly to the above two-dimensional case, define eight triple integrals:

$$I_t^{(\delta,\varepsilon,\eta)} = t^{-l-q-s} \times \int\limits_{[\delta]} \Bigg(\int\limits_{[\varepsilon]} \Bigg(\int\limits_{[\eta]} \frac{x^j(1-x)^h\, y^k(1-y)^l z^p(1-z)^q(t-x)^{w+1}}{\big(x(1-y)+yt\big)^{j+k-m+1}\big(x(1-z)+zt\big)^{j+p-r+1}}\,\mathrm{d}z\Bigg)\,\mathrm{d}y\Bigg)\,\mathrm{d}x,$$

where δ,ε,η are either 0 or 1, and where $\int_{[0]}$ means $\int_0^1$, and $\int_{[1]} \cdots \mathrm{d}x$ (resp. $\mathrm{d}y, \mathrm{d}z$) means $\frac{1}{2\pi i}\oint_{|x-t|=\sigma} \cdots \mathrm{d}x$ (resp. $\frac{1}{2\pi i}\oint_{|y-x/(x-t)|=\varrho} \cdots \mathrm{d}y$, $\frac{1}{2\pi i}\oint_{|z-x/(x-t)|=\tau} \cdots \mathrm{d}z$), for any small $\varrho,\sigma,\tau > 0$.

Let $\alpha = \max\{k+q+r,\, l+q+s,\, j+k+p,\, l+m+p,\, k+l+p+q-w\}$, $\beta = \max\{0,\, k+l+p+q-w-h\}$, and let

$$\begin{aligned} I_t^{(0)} &= I_t^{(0,0,0)} - \big(I_t^{(0,0,1)} + I_t^{(0,1,0)}\big)\log t + I_t^{(0,1,1)}\log^2 t,\\ I_t^{(1)} &= I_t^{(1,0,0)} - \big(I_t^{(1,0,1)} + I_t^{(1,1,0)}\big)\log t + I_t^{(1,1,1)}\log^2 t. \end{aligned}$$

Then

$$t^\alpha(t-1)^\beta I_t^{(0)} = P(t) + R(t)\,\mathrm{Li}_2(1/t) + S(t)\,2\mathrm{Li}_3(1/t),$$

with $P(t), R(t), S(t) \in \mathbb{Q}[t]$ polynomials with controlled degrees and denominators. Moreover

$$I_t^{(1,0,0)} = 0, \quad R(t) = -t^\alpha(t-1)^\beta\big(I_t^{(1,0,1)} + I_t^{(1,1,0)}\big), \quad S(t) = -t^\alpha(t-1)^\beta I_t^{(1,1,1)},$$

so that

$$\begin{cases} t^\alpha(t-1)^\beta I_t^{(0)} = P(t) + Q(t)\,\mathrm{Li}_1(1/t) + R(t)\,\mathrm{Li}_2(1/t) + S(t)\,2\mathrm{Li}_3(1/t)\\ t^\alpha(t-1)^\beta I_t^{(1)} = \qquad - Q(t) \qquad + R(t)\log t \qquad - S(t)\log^2 t, \end{cases}$$

with $Q(t) = 0$, is a solution to a Padé-type approximation problem similar to (4) for $n = 3$.

References

[1] F. Beukers, *The values of polylogarithms*, in: Topics in classical number theory, Colloq. Math. Soc. János Bolyai **34**, Budapest (1981), 219–228.

[2] S. Fischler and T. Rivoal, *Approximants de Padé et séries hypergéométriques équilibrées*, J. Math. Pures Appl. (9) **82** (2003), 1369–1394.

[3] G. Rhin and C. Viola, *The permutation group method for the dilogarithm*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (5) **4** (2005), 389–437.

[4] G. Rhin and C. Viola, *Multiple integrals and linear forms in zeta-values*, Funct. Approx. Comment. Math. **37** (2007), 429–444.

Rational approximation to real points on plane algebraic curves

Damien Roy

There are many ways in which one can measure how well a real point $\underline{\xi} = (\xi_1, \dots, \xi_n) \in \mathbb{R}^n$ can be approximated by rational points from $\mathbb{Q}^n$. In this report, we deal with the quantity $\lambda(\underline{\xi})$ defined as the supremum of all $\lambda \geq 0$ such that the system of inequalities

$$|x_0| \leq X, \quad |x_0\xi_1 - x_1| \leq X^{-\lambda}, \ \dots, \ |x_0\xi_n - x_n| \leq X^{-\lambda}$$

admits a non-zero solution $\mathbf{x} = (x_0, x_1, \dots, x_n) \in \mathbb{Z}^{n+1}$ for each sufficiently large $X > 1$. For such a solution with $x_0 \neq 0$, the point $(x_1/x_0, \dots, x_n/x_0) \in \mathbb{Q}^n$ is indeed an approximation to $\underline{\xi}$. An application of Dirichlet box principle yields $\lambda(\underline{\xi}) \geq 1/n$ for any $\underline{\xi} \in \mathbb{R}^n$, while metrical arguments show that $\lambda(\underline{\xi}) = 1/n$ for all $\underline{\xi} \in \mathbb{R}^n$ outside of a set of Lebesgue measure zero. So, the points $\underline{\xi} \in \mathbb{R}^n$ with $\lambda(\underline{\xi}) > 1/n$ are somewhat exceptional. They are those for which one can do much better than predicted by the box principle in approximating $\underline{\xi}$ in the above sense. A trivial situation in which this happens is when $1, \xi_1, \dots, \xi_n$ are linearly dependent over $\mathbb{Q}$. Then, upon denoting by s the dimension of the vector subspace of $\mathbb{R}$ spanned over $\mathbb{Q}$ by these numbers, we find that $\lambda(\underline{\xi}) \geq 1/(s-1)$. Finally, the exponent $\lambda(\underline{\xi})$ is interesting only when $n \geq 2$ because, in the case $n = 1$, we have $\lambda(\xi) = 1$ for each irrational real number ξ.

Our work is motivated by the following result [1] where $\gamma := (1+\sqrt{5})/2 = 1.618\dots$ stands for the Golden ratio.

Theorem 1 (Davenport and Schmidt, 1969)**.** *Let $\xi \in \mathbb{R}$ with $1, \xi, \xi^2, \dots, \xi^n$ linearly independent over $\mathbb{Q}$. Then*

$$\lambda(\xi, \xi^2, \dots, \xi^n) \leq \lambda_n := \begin{cases} 1/\gamma \cong 0.618 & \text{if } n = 2, \\ 1/2 & \text{if } n = 3, \\ 1/\lfloor n/2 \rfloor & \text{if } n \geq 4. \end{cases}$$

In [2], M. Laurent showed that this estimate remains true with $\lambda_n = 1/\lceil n/2 \rceil$ for each $n \geq 3$. In the case $n = 3$, the best known estimate up to now is $\lambda_3 \leq (1 + 2\gamma - \sqrt{1+4\gamma^2})/2 \cong 0.4245$ (see [7]). A consequence of Theorem 1 and the starting point of the paper [1] of Davenport and Schmidt is the fact that, for any ξ as in Theorem 1 and any $\tau < 1 + (1/\lambda_n)$, there are infinitely many algebraic integers α of degree $\leq n+1$ such that $|\xi - \alpha| \leq H(\alpha)^{-\tau}$ where $H(\alpha)$ stands for the naive height of α namely the largest absolute value of the coefficients of its irreducible polynomial over $\mathbb{Z}$. Thus, if one could prove for example that the optimal value for λ_n is close to $1/n$, then the above would hold with τ close to n and this would represent a major progress towards the problem of Wirsing. However, at present, we only know that, for $n = 2$, the value $\lambda_2 = 1/\gamma$ is optimal and that, in the corresponding result of approximation by cubic algebraic integers, the condition $\tau < 1 + \gamma$ cannot be strengthened [4, 5, 6].

The points $(\xi, \xi^2, \dots, \xi^n)$ with $\xi \in \mathbb{R}$ form an irreducible closed algebraic subset $\mathcal{C}$ of $\mathbb{R}^n$ of dimension one defined over $\mathbb{Q}$. The optimal value for λ_n which we are looking for is simply the supremum of $\lambda(\xi,\dots,\xi^n)$ over all points $(\xi,\dots,\xi^n)$ of $\mathcal{C}$ whose coordinates together with 1 are linearly independent over $\mathbb{Q}$. Thus it is natural to extend the problem to all algebraic curves of that sort, in the hope that, in the process, we can gain new ideas that will help solve the initial question. Since it is easier to work with projective curves, we first recall that the above notion of exponent of approximation extends naturally to points of the projective space $\mathbb{P}^n(\mathbb{R})$. For such a point $\Xi = (\xi_0 : \xi_1 : \cdots : \xi_n)$, the exponent $\lambda(\Xi)$ is defined as the supremum of all $\lambda \geq 0$ such that

$$\|\mathbf{x}\| \leq X, \qquad \|\mathbf{x} \wedge (\xi_0,\dots,\xi_n)\| \leq X^{-\lambda}$$

has a solution $\mathbf{x} \in \mathbb{Z}^{n+1} \setminus \{0\}$ for each sufficiently large $X \geq 1$. Then, for any $(\xi_1,\dots,\xi_n) \in \mathbb{R}^n$, we have

$$\lambda(1 : \xi_1 : \cdots : \xi_n) = \lambda(\xi_1,\dots,\xi_n).$$

Definition. Let $\mathcal{C}$ be a closed algebraic subset of $\mathbb{P}^n(\mathbb{R})$ of dimension 1, defined over $\mathbb{Q}$ and irreducible over $\mathbb{Q}$. Suppose that $\mathcal{C}$ is not contained in a proper linear subspace of $\mathbb{P}^n(\mathbb{R})$ defined over $\mathbb{Q}$, and let $\mathcal{C}^{li}$ denote the set of points Ξ in $\mathcal{C}$ which admit a set of $\mathbb{Q}$-linearly independent homogeneous coordinates. Then, we set

$$\lambda(\mathcal{C}) := \sup\{\lambda(\Xi)\,;\, \Xi \in \mathcal{C}^{li}\}.$$

The first result on which we want to report is the fact that $\lambda(\mathcal{C}) = 1/\gamma$ for each conic $\mathcal{C}$ in $\mathbb{P}^2(\mathbb{R})$ that is defined and irreducible over $\mathbb{Q}$. More precisely, we have the following statement [8].

Theorem 2. *Let $\varphi \in \mathbb{Q}[x_0,x_1,x_2]$ be irreducible and homogeneous of degree 2. Suppose that the set $\mathcal{C}$ of zeros of φ in $\mathbb{P}^2(\mathbb{R})$ is infinite. Then:*

(a) $\lambda(\Xi) \leq 1/\gamma$ for any $\Xi \in \mathcal{C}^{li}$,

(b) $\{\Xi \in \mathcal{C}^{li}\,;\, \lambda(\Xi) = 1/\gamma\}$ is a countably infinite set.

For example, for $\varphi = x_0x_2 - x_1^2$, we find $\mathcal{C} = \{(1 : \xi : \xi^2)\,;\, \xi \in \mathbb{R}\} \cup \{(0 : 0 : 1)\}$. Thus

$$\mathcal{C}^{li} = \{(1 : \xi : \xi^2)\,;\, \xi \in \mathbb{R},\ [\mathbb{Q}(\xi) : \mathbb{Q}] > 2\},$$

and we recover in (a) the result of Davenport and Schmidt mentioned above for the case $n = 2$, while (b) is essentially the main result of [6].

Another example is provided by the zero set $\mathcal{C}$ of $\varphi = 2x_0^2 - x_1^2$, for which

$$\mathcal{C}^{li} = \{(1 : \pm\sqrt{2} : \xi)\,;\, \xi \in \mathbb{R} \setminus \mathbb{Q}(\sqrt{2})\}.$$

According to Theorem 2, we have $\lambda(\mathcal{C}) = 1/\gamma$. However, the main result of [7] is slightly more precise than Theorem 2 and yields:

(a) For any $\xi \in \mathbb{R}\setminus\mathbb{Q}(\sqrt{2})$, there exists $c = c_1(\xi) > 0$ such that the inequalities

$$|x_0| \leq X,\ |x_0\sqrt{2} - x_1| \leq cX^{-1/\gamma},\ |x_0\xi - x_2| \leq cX^{-1/\gamma}, \tag{1}$$

have no solution $(x_0,x_1,x_2) \in \mathbb{Z}^3 \setminus \{0\}$ for arbitrarily large values of X.

(b) There exists $\xi \in \mathbb{R}\setminus\mathbb{Q}(\sqrt{2})$ and $c = c_2(\xi) > 0$ such that (1) have a solution for each $X \geq 1$. The set of these numbers ξ is countably infinite.

Theorem 2 exhausts the set of all curves $\mathcal{C}$ for which we are able to compute $\lambda(\mathcal{C})$ at present. However, the last example suggests the problem of determining

$$\sup\{\lambda(\omega_1 : \cdots : \omega_n : \xi)\,;\, \xi \in \mathbb{R} \setminus K\}$$

where K is a number field of degree n over $\mathbb{Q}$ and $(\omega_1, \ldots, \omega_n)$ is a basis of K over $\mathbb{Q}$. In joint work with Stéphane Lozier [3], we prove the following estimate.

Theorem 3 (with S. Lozier)**.** *For any $\xi \in \mathbb{R}$ such that $1, \xi, \xi^3$ are linearly independent over $\mathbb{Q}$, we have*

$$\lambda(1 : \xi : \xi^3) \leq \frac{2(9+\sqrt{11})}{35} = 0.7038\ldots$$

i.e. the cubic $\mathcal{C} : x_0^2 x_2 - x_1^3 = 0$ in $\mathbb{P}^2(\mathbb{R})$ has $\lambda(\mathcal{C}) \leq 0.7038\ldots$.

The upper bound for $\lambda(1 : \xi : \xi^3)$ in the above result is not optimal and the method that we describe in [3] allows to reduce it, possibly down to $\lambda(1 : \xi : \xi^3) \leq (1 + 3\sqrt{5})/2 \cong 0.7007$ but we have not been able to go this far.

The proof of Theorem 2 is based on ideas of [1, 6]. A conic as in the statement of this theorem contains either infinitely many points of $\mathbb{P}^2(\mathbb{Q})$, or at most one such point. In the first case, it can be transformed into the conic with equation $x_0x_2 - x_1^2 = 0$ by a linear automorphism of $\mathbb{P}^2(\mathbb{R})$ defined over $\mathbb{Q}$. As the exponent λ is invariant under such transformation, the conclusion of the theorem follows immediately from [1, 6] in that case. In the complementary case, some simplifications occur in the proof of Part (a) due to the finiteness of the set of rational points on the conic $\mathcal{C}$. However, the construction of "extremal" points for Part (b) requires additional arguments with respect to [6].

References

[1] H. Davenport, W. M. Schmidt, *Approximation to real numbers by algebraic integers*, Acta Arith. **15** (1969), 393–416.

[2] M. Laurent, *Simultaneous rational approximation to the successive powers of a real number*, Indag. Math. (N.S.) **11** (2003), 45–53.

[3] S. Lozier and D. Roy, *Simultaneous approximation to a real number and to its cube*, submitted.

[4] D. Roy, *Approximation simultanée d'un nombre et de son carré*, C. R. Acad. Sci., Paris, ser. I **336** (2003), 1–6.

[5] D. Roy, *Approximation to real numbers by cubic algebraic integers (II)*, Ann. of Math. **158** (2003), 1081–1087.

[6] D. Roy, *Approximation to real numbers by cubic algebraic integers I*, Proc. London Math. Soc. **88** (2004), 42–62.

[7] D. Roy, *On simultaneous rational approximations to a real number, its square, and its cube*, Acta Arith. **133** (2008), 185–197.

[8] D. Roy, *Rational approximation to real points on conics*, Ann. Inst. Fourier (Grenoble), to appear.

Effective results for Diophantine equations over finitely generated domains

Jan-Hendrik Evertse
(joint work with Attila Bérczes, Kálmán Győry)

Let $A = \mathbb{Z}[z_1, \ldots, z_q] \supset \mathbb{Z}$ be an integral domain which is finitely generated over $\mathbb{Z}$. Then

$$A \cong \mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_s),$$

where $f_1, \ldots, f_s$ is a system of generators for the ideal of $f \in \mathbb{Z}[X_1, \ldots, X_r]$ with $f(z_1, \ldots, z_r) = 0$. We want to give effective finiteness results for certain classes of Diophantine equations with unknowns taken from the domain A.

To state our results, we need some terminology. Given $a \in A$, we call $\widetilde{a} \in \mathbb{Z}[X_1, \ldots, X_r]$ a *representative* for a if $\widetilde{a}(z_1, \ldots, z_s) = a$. There exist algorithms with which one can decide for given $f, f_1, \ldots, f_s \in \mathbb{Z}[X_1, \ldots, X_r]$ whether $f \in (f_1, \ldots, f_s)$ (see Simmons [13, 1970], Aschenbrenner [1, 2004]). With the help of this, one can decide effectively whether two polynomials $f, g \in \mathbb{Z}[x_1, \ldots, X_r]$ represent the same element of A.

For $f \in \mathbb{Z}[X_1, \ldots, X_r]$, let $\deg f$ denote its total degree and $h(f)$ its logarithmic height (i.e., the maximum of the logarithms of the absolute values of its coefficients), and define its size $s(f) := \max(1, \deg f, h(f))$. Then we define the size of $x \in A$ by the minimum of the quantities $s(\widetilde{x})$, taken over all representatives $\widetilde{x} \in \mathbb{Z}[X_1, \ldots, X_r]$ for x.

Notice that if $F \in A[Y_1, \ldots, Y_t]$ is a polynomial with coefficients in A, and we are given $\widetilde{F} \in \mathbb{Z}[X_1, \ldots, X_r][Y_1, \ldots, Y_t]$ whose coefficients represent those of F, then in order to determine effectively all solutions of the equation $(*)$ $F(y_1, \ldots, y_t) = 0$ in $y_1, \ldots, y_t \in A$, it suffices to give a number C such that $\max_i s(y_i) \leq C$ for all solutions $(y_1, \ldots, y_t)$ of $(*)$. Indeed, one simply needs to check for all polynomials $\widetilde{y_1}, \ldots, \widetilde{y_t} \in \mathbb{Z}[X_1, \ldots, X_r]$ of size $\leq C$ whether $\widetilde{F}(\widetilde{y_1}, \ldots, \widetilde{y_t}) \in (f_1, \ldots, f_s)$.

Recently, Győry and the author [8, 2011] proved the following result on unit equations over A in two unknowns:

Let a, b, c be non-zero elements of A and let be given representatives $\widetilde{a}, \widetilde{b}, \widetilde{c}$ for a, b, c. Suppose that $f_1, \ldots, f_s$ and $\widetilde{a}, \widetilde{b}, \widetilde{c}$ have total degrees at most d and logarithmic heights at most h where $d, h \geq 1$. Then for the solutions x, y of

$$ax + by = c \quad \text{in } x, y \in A^*$$

we have

$$s(x), s(x^{-1}), s(y), s(y^{-1}) \leq \exp\left\{(2d)^{\kappa^r}(h+1)\right\}$$

where κ is an effectively computable absolute constant.

The method of proof of this result can be applied to other classes of Diophantine equations as well. To illustrate this, we give some effective results for Thue equations and hyper- and superelliptic equations over A, obtained jointly with Bérczes and Győry. We always use κ to denote an effectively computable absolute constant, but at each occurrence, its value may be different.

Let $F(X,Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_0Y^n \in A[X,Y]$ be a binary form of degree $n \geq 3$ without multiple factors, and let $b \in A \setminus \{0\}$. Consider the equation

$$F(x,y) = b \quad \text{in } x, y \in A. \tag{1}$$

Baker [2, 1968] gave in the case $A = \mathbb{Z}$ an effective proof that (1) has only finitely many solutions. This was extended by Coates [7, 1968/69] to the case $A = \mathbb{Z}[(p_1 \cdots p_t)^{-1}]$ where the p_i are distinct primes and by Kotov and Sprindzhuk [10, 1973] to the case that A is the ring of S-integers in a number field. Győry [9, 1983] extended this effective finiteness result further to integral domains of the special shape $\mathbb{Z}[z_1, \ldots, z_q, w, g^{-1}]$, where $z_1, \ldots, z_q$ are algebraically independent, w is integral over $A_0 := \mathbb{Z}[z_1, \ldots, z_q]$, and $g \in A_0$. In his proof, Győry developed a specialization method, which we managed to extend to arbitrary finitely generated domains. This led to the following general result for Thue equations. As before, A is an integral domain containing $\mathbb{Z}$, isomorphic to $\mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_s)$.

Theorem 1 (Bérczes, E., Győry). *Let $\widetilde{a_0}, \ldots, \widetilde{a_n}, \widetilde{b}$ be representatives for the coefficients $a_0, \ldots, a_n$ of F and of b, and assume that these representatives, as well as $f_1, \ldots, f_s$, have total degrees $\leq d$ and logarithmic heights at most h. Then for the solutions of* (1) *we have*

$$s(x), s(y) \leq \exp\left\{(n!)^3 n^5 (2d)^{\kappa^r}(h+1)\right\}.$$

Now let $F(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in A[X]$, $b \in A \setminus \{0\}$, $m \in \mathbb{Z}_{\geq 2}$ and consider the hyper-/superelliptic equation

$$by^m = F(x) \quad \text{in } x, y \in A. \tag{2}$$

Assume that F has no multiple roots, and that F has degree $n \geq 3$ if $m = 2$ and degree $n \geq 2$ if $m \geq 3$. Again Baker[3, 1969] was the first to give an effective finiteness proof for the set of solutions of (2), in the case $A = \mathbb{Z}$. This was extended by Brindza [4, 1984] to the case that A is the ring of S-integers of a number field, and further[6, 1989] to the special class of finitely generated domains mentioned above considered by Győry. In the case $A = \mathbb{Z}$, Schinzel and Tijdeman [12, 1976] proved that if (2) has a solution $x, y \in \mathbb{Z}$ with $y \neq 0, \pm 1$, then m is bounded above by an effectively computable number depending only on F and b. Brindza [5, 1987] extended this to the case that A is the ring of S-integers in a number field, and Végső [14, 1994] to the class of domains considered by Győry.

Theorem 2 (Bérczes, E., Győry). *Let $\widetilde{a_0}, \ldots, \widetilde{a_n}, \widetilde{b}$ be representatives for the coefficients $a_0, \ldots, a_n$ of F and of b, and assume that these representatives, as well as $f_1, \ldots, f_s$, have total degrees $\leq d$ and logarithmic heights at most h. Then for the solutions of* (2) *we have*

$$s(x), s(y) \leq \exp\left\{m^2 n^5 (2d)^{\kappa^r}(h+1)\right\}.$$

Further, if (2) *has a solution $x, y \in A$ with y not equal to* 0 *or to a root of unity, then*

$$m \leq \exp\left\{n^5 (2d)^{\kappa^r}(h+1)\right\}.$$

We sketch the proof of Theorem 1; the proof of Theorem 2 is essentially similar. Let as before $A = \mathbb{Z}[z_1, \ldots, z_r] \supset \mathbb{Z}$ be an integral domain. Assume that $z_1, \ldots, z_q$ are linearly independent, and that $z_{q+1}, \ldots, z_r$ are algebraic over $K_0 := \mathbb{Q}(z_1, \ldots, z_q)$. Choose $w \in A$ integral over $A_0 := \mathbb{Z}[z_1, \ldots, z_q]$ and choose $g \in A_0$ such that $A \subseteq B := \mathbb{Z}[z_1, \ldots, z_q, w, g^{-1}]$. Assume that w has degree D over K_0. Given $\mathbf{u} = (u_1, \ldots, u_q) \in \mathbb{Z}^q$ with $g(\mathbf{u}) \neq 0$, we can define a specialization homomorphism $\varphi_{\mathbf{u}} : B \to \overline{\mathbb{Q}}$ by mapping z_i to u_i for $i = 1, \ldots, q$. Then $\varphi_{\mathbf{u}}$ maps the Thue equation (1) over A to a Thue equation ($1_{\mathbf{u}}$) over the ring of $S_{\mathbf{u}}$-integers $O_{S_{\mathbf{u}}}$ in a number field $K_{\mathbf{u}}$, where both the number field $K_{\mathbf{u}}$ and the set of places $S_{\mathbf{u}}$ may depend on $\mathbf{u}$.

Now let $x, y \in A$ be a solution of (1). We can express x as $\sum_{i=0}^{D-1} P_i w^i / Q$, where $P_0, \ldots, P_{D-1}, Q \in \mathbb{Z}[z_1, \ldots, z_q]$. Using Mason's effective result for Thue equations over function fields [11, 1984] one can estimate the degrees of $P_0, \ldots, P_{D-1}, Q$. By applying Baker's method to the Thue equations ($1_{\mathbf{u}}$) for 'many' $\mathbf{u} \in \mathbb{Z}^q$, and then using linear algebra, one can estimate the coefficients of the P_i and Q. Up to this point, this outlines Győry's specialization method mentioned above. Using a recent effective result by Aschenbrenner [1, 2004] for systems of inhomogeneous linear equations over polynomial rings over $\mathbb{Z}$, one can estimate the size $s(x)$ of x in terms of the total degrees and heights of the P_i and Q. The size $s(y)$ of the other unknown is estimated in the same way.

The above method of proof can by applied to various other classes of Diophantine equations. we would like to finish with an open problem. Consider the Thue-Mahler equation over an arbitrary finitely generated domain A,

$$F(x, y) \in A^* \quad \text{in } x, y \in A, \tag{3}$$

where $F \in A[X, Y]$ is a binary form of degree ≥ 3 without multiple factors. One can show that (3) has finitely many solutions $(x_1, y_1), \ldots, (x_l, y_l)$, such that every other solution of (3) is expressable in the form $u(x_i, y_i)$ with $u \in A^*$, $i \in \{1, \ldots, l\}$. Given an arbitrary finitely generated domain A, can one determine such (x_i, y_i) effectively?

References

[1] M. Aschenbrenner, *Ideal membership in polynomial rings over the integers*, J. Amer. Math. Soc. **17** (2004), 407–442.

[2] A. Baker, *Contributions to the theory of Diophantine equations*, Philos. Trans. Roy. Soc. London, Ser. A **263**, 173–208.

[3] A. Baker, *Bounds for the solutions of the hyperelliptic equation*, Proc. Cambridge Philos. Soc. **65** (1969), 439–444.

[4] B. Brindza, *On S-integral solutions of the equation $y^m = f(x)$*, Acta Math. Hung. **44** (1984), 133–139.

[5] B. Brindza, *Zeros of polynomials and exponential diophantine equations*, Compos. Math. **61** (1987), 137–157.

[6] B. Brindza, *On the equation $f(x) = y^m$ over finitely generated domains*, Acta Math. Hung. **53** (1989), 377–383.

[7] J. Coates, *An effective p-adic analogue of a theorem of Thue*, Acta Arith. **15** (1968/69), 279–305.

[8] J.-H. Evertse, K. Győry, *Effective results for unit equations over finitely generated integral domains*, submitted for publication, arXiv:1107:5756.
[9] K. Győry, *Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated domains*, Acta Math. Hung. **42** (1983), 45–80.
[10] S.V. Kotov, V.G. Sprindzhuk, *An effective analysis of the Thue-Mahler equation in relative fields* (Russian), Dokl. Akad. Nauk. BSSR **17** (1973), 393–395; 477.
[11] R.C. Mason, *Diophantine Equations over Function Fields*, London Math. Soc. Lecure Notes Series 96, Cambridge Univ. Press, 1984.
[12] A. Schinzel, R. Tijdeman, *On the equation $y^m = P(x)$*, Acta Arith. **31** (1976), 199–204.
[13] H. Simmons, *The solution of a decision problem for several classes of rings*, Pacific J. Math. **34** (1970), 547–557.
[14] J. Végső, *On superelliptic equations*, Publ. Math. Debrecen **44** (1994), 183–187.

On three problems in Diophantine approximation

Nikolay Moshchevitin

We discuss three classes of problems in Diophantine approximation.

The first one is related to W.M. Schmidt's question concerning Diophantine approximation with positive integers. Recently we constructed a counterexample to a conjecture by W.M. Schmidt by proving that there exist two algebraically independent real numbers θ_1, θ_2 such that

$$\inf_{m_1, m_2 \in \mathbb{Z}_+} \max(m_1, m_2)^\sigma \cdot ||m_1\theta_1 + m_2\theta_2|| > 0$$

with $\sigma = 1.94696^+$. There are different open questions concerning various inequalities involving Diophantine exponents for ordinary and uniform Diophantine approximations and for approximations with positive integers.

The second class of problems deals with Jarník's inequalities for uniform and ordinary Diophantine exponents $\hat{\omega}$ and ω. Recently W.M. Schmidt and L. Summerer got an important result in Geometry of Numbers. This result enables one to improve old Jarník's theorem in the general case. We have better results in the case of simultaneous approximations to three real numbers and in the case of one linear form in three variables.

The third class of problems deals with Minkowski question mark function $?(x)$. The simplest problem is as follows. *How many solutions has the equation $?(x) = x$?*

Research is supported by the grant RFBR No. 12-01-00681-a and by the grant of Russian Government, project 11. G34.31.0053.

Inhomogeneous approximation and lattice orbits

Michel Laurent
(joint work with Arnaldo Nogueira)

Our starting point is the celebrated Minkowski Theorem on inhomogeneous approximation.

Theorem 1 (Minkowski)**.** *Let ξ be an irrational real number ξ and let y be a real number not belonging to $\mathbb{Z}\xi + \mathbb{Z}$. There exist infinitely many pairs of integers p, q such that*

$$|q\xi + p - y| \leq \frac{1}{4|q|}.$$

Minkowski Theorem holds for every real point (ξ, y) as above. An other classical related result is the following metrical statement due to Cassels which is valid only for almost every point (ξ, y). Note that no monotony condition is assumed for the approximating function ψ.

Theorem 2 (Cassels)**.** *Let $\psi : \mathbb{N} \mapsto [0, 1/2]$ be a function such that*

$$\sum_{\ell \geq 1} \psi(\ell) = +\infty.$$

Then, for almost all pairs (ξ, y) of real numbers there exist infinitely many integer points (p, q) such that

$$|q\xi + p - y| \leq \psi(|q|). \tag{1}$$

The goal of the talk is to discuss similar results where we moreover require that the pairs of integers p, q be coprime. In this direction, Chalk and Erdős [1] have proved the following statement:

Theorem 3 (Chalk & Erdős)**.** *Let ξ be an irrational real number and let y be a real number. There exists an absolute constant c such that the inequality*

$$|q\xi + p - y| \leq \frac{c(\log|q|)^2}{|q|(\log\log|q|)^2} \tag{2}$$

holds for infinitely many pairs of coprime integers (p, q).

The optimality of the Chalk-Erdős Theorem remains unclear. We address the following

Problem. *Can we replace the approximating function $\psi(\ell) = c(\log \ell)^2/\ell(\log\log \ell)^2$ occurring in (2) by a smaller one, possibly $\psi(\ell) = c\,\ell^{-1}$?*

Putting now $\psi(\ell) = c\ell^{-1/2}$ and using our results [2] on effective density for $SL(2, \mathbb{Z})$-orbits in $\mathbb{R}^2$, we construct in [3] pairs of solutions of (1) forming a matrix of determinant one.

Theorem 4. *Let ξ be an irrational real number and let y be a real number. There exist infinitely many integer quadruples (p_1, q_1, p_2, q_2) satisfying*

$$q_1 p_2 - p_1 q_2 = 1$$

and

$$|q_i\xi + p_i - y| \le \frac{c}{\max(|q_1|, |q_2|)^{1/2}} \le \frac{c}{\sqrt{|q_i|}}, \quad (i = 1, 2), \tag{3}$$

with $c = 2\sqrt{3}\max(1, |\xi|)^{1/2}|y|^{1/2}$.

The estimate (3) is best possible, up to the value of the constant c.

Concerning metrical results analogue to Theorem 2, we obtain in [3] the following two theorems.

Theorem 5. *Let $\psi : \mathbb{N} \mapsto \mathbb{R}^+$ be a function. Assume that ψ is non-increasing, tends to 0 at infinity and that for every positive integer c there exists a positive real number c_1 satisfying*

$$\psi(c\,\ell) \ge c_1 \psi(\ell), \quad \forall \ell \ge 1.$$

Furthermore assume that

$$\sum_{\ell \ge 1} \psi(\ell) = +\infty.$$

Then, for almost all pairs (ξ, y) of real numbers there exist infinitely many primitive points (p, q) such that

$$|q\xi + p - y| \le \psi(|q|).$$

It should be interesting to weaken the hypotheses on the approximation function ψ occurring in Theorem 5. A question which naturally arises in view of Theorem 5 is to understand what happens on each fiber when we fix either ξ or y. In this direction, here is a partial result:

Theorem 6. *Let ξ be an irrational number and let $(p_k/q_k)_{k \ge 0}$ be the sequence of its convergents. Assume that the series*

$$\sum_{k \ge 0} \frac{1}{\max(1, \log q_k)}$$

diverges. Then for almost every real number y there exist infinitely many primitive points (p, q) satisfying

$$|q\xi + p - y| \le \frac{2}{|q|}.$$

References

[1] J. H. H. Chalk and P. Erdős, *On the distribution of primitive lattice points in the plane*, Canad. Math. Bull. **2** (1959), 91–96.

[2] M. Laurent and A. Nogueira, *Approximation to points in the plane by $SL(2,\mathbb{Z})$-orbits*, J. London Math. Soc. **85** (2012), 409–429.

[3] M. Laurent and A. Nogueira, *Inhomogeneous approximation with coprime integers and lattice orbits*, to appear in Acta Arithmetica.

Symmetry in Legendre-type polynomials and Diophantine approximation of logarithms

Raffaele Marcovecchio

This research is devoted to the study of Diophantine approximation of numbers of the form $\log(1+\frac{1}{k})$, where $k \geq 1$ is an integer. Legendre polynomials are Padé approximations to the function $\log(1-z)$ at $z=0$, so that they are naturally related to the Diophantine properties of $\log(1+\frac{1}{k})$. For this reason simple integrals involving Legendre and Legendre-type polynomials have been used by several authors (Alladi-Robinson [1], Rukhadze [9], Hata [3], ...) in order to find new irrationality measures of $\log(1+\frac{1}{k})$. We recall that μ is an irrationality measure of the irrational α if for any $\varepsilon > 0$ there exists a positive integer $q(\varepsilon)$ such that

$$\left|\alpha - \frac{p}{q}\right| > q^{-\mu-\varepsilon}$$

for all integers $q \geq q(\varepsilon)$ and for all $p \in \mathbb{Z}$.

An alternative approach was introduced by Viola [10], making use of Euler's integral representation of the hypergeometric function (note that ${}_2F_1(1,1;2;z) = -\frac{\log(1-z)}{z}$). Since the integrand is a rational function, this representation, together with a change of variable in this (simple real) integral, induces a permutation group acting on the integer exponents appearing in this rational function. This method was extended by Amoroso-Viola [2] to find new approximation measures of logarithms of algebraic numbers.

In connection with new non-quadraticity measures of $\log(1+\frac{1}{k})$, Hata [4] introduced a family of double complex integrals, again involving Legendre-type polynomials. We recall that ν is a non-quadraticity measure of the non-quadratic number β if for any $\varepsilon > 0$ there exists a positive integer $H_0(\varepsilon)$ such that

$$|\beta - Q| > H(Q)^{-\nu-\varepsilon}$$

for all quadratic numbers Q whose height $H(Q)$ is at least $H_0(\varepsilon)$.

In [5] I proposed a family of double complex integrals somehow related to Hata's. These integrals, however, do not involve Legendre-type polynomials, but instead are equipped with a permutation group acting on the parameters appearing in the rational function at the integrand. Just as in Viola's and Rhin-Viola's papers some generators of this permutation group are induced by suitable changes of variables, some other generators are induced by Euler's integral representation of the hypergeometric function and its symmetry properties, so that the permutation group has two different kinds of generators. Each permutation is naturally associated with a certain quotient of factorials. The sets of permutations associated with the same quotient are exactly the left cosets of the whole permutation group with respect to the subgroup generated by permutations induced by changes of variables only. For instance, I proved that 3.57455390... is an irrationality measure of $\log 2$, and 15.65142024... is a non-quadraticity measure of $\log 2$. Recently, Viola and myself [6] extended this method to logarithms of algebraic numbers, thus improving some results by Amoroso-Viola [2].

In 2010 Nesterenko [7] gave a considerably simplified proof of the above irrationality measure of $\log 2$. His method makes use of integrals of Mellin-Barnes's type, as in Nesterenko's proof in 1996 of Apèry's theorem on the irrationality of $\zeta(3)$. Along the same lines Polyanskii [8] gave a similar proof of the above non-quadraticity measure of $\log 2$.

The present research intends to introduce a third approach to the construction of a sequence of rational approximations to $\log(1+\frac{1}{k})$ yielding the above irrationality measure of $\log 2$. This new construction involves a family of Legendre-type polynomials with suitable symmetry properties.

Let $(\boldsymbol{p};\boldsymbol{q}) = (p_1,\dots,p_n;q_1,\dots,q_n)$, where $p_i, q_i \geq 0$ are integers. Let $\mathcal{L}_n(\boldsymbol{p};\boldsymbol{q};z)$ be the polynomial recursively defined by $\mathcal{L}_0(z)=1$ and

$$\mathcal{L}_{n+1}(\boldsymbol{p},p_{n+1};\boldsymbol{q},q_{n+1};z) \\ = z^{q_{n+1}}(1-z)^{p_{n+1}} D_{p_{n+1}+q_{n+1}}\big(z^{p_{n+1}}(1-z)^{q_{n+1}}\mathcal{L}_n(\boldsymbol{p};\boldsymbol{q};z)\big),$$

where $D_m = \frac{1}{m!}(\frac{\mathrm{d}}{\mathrm{d}z})^m$. For example

$$\mathcal{L}_1(p_1;q_1;z) = (-z)^{q_1}(1-z)^{p_1}.$$

The polynomials

$$\mathcal{L}_2(p_1,p_2;q_1,q_2;z) = (-1)^{q_1} z^{q_2}(1-z)^{p_2} D_{p_2+q_2}\big(z^{p_2+q_1}(1-z)^{p_1+q_2}\big)$$

have the property that their coefficients have a large common divisor when p_1, p_2, q_1, q_2 are not all equal, and for this reason they were used in Rukhadze's and Hata's papers. It is not difficult to see that the polynomial

$$\mathcal{L}_n(p_1,\dots,p_n;q_1,\dots,q_n;z)\prod_{1\leq i\leq n}(p_i+q_i)!$$

is a bisymmetric function of $p_1,\dots,p_n$ and of $q_1,\dots,q_n$. In particular, $\mathcal{L}_n(\boldsymbol{p};\boldsymbol{q};z)$ is a symmetric function of $(p_1,q_1),\dots,(p_n,q_n)$.

In my talk I discuss how to use the polynomials

$$\mathcal{L}_3(p_1,p_2,p_3;q_1,q_2,q_3;z) \\ = (-1)^{q_1} z^{q_3}(1-z)^{p_3} D_{p_3+q_3}\Big(z^{p_3+q_2}(1-z)^{p_2+q_3} D_{p_2+q_2}\big(z^{p_2+q_1}(1-z)^{p_1+q_2}\Big)$$

to construct the same approximations to logarithms as in my paper [5].

References

[1] K. Alladi and M. L. Robinson, *Legendre polynomials and irrationality*, J. Reine Angew. Math. **318** (1980), 137–155.

[2] F. Amoroso and C. Viola, *Approximation measures for logarithms of algebraic numbers*, Ann. Scuola Norm. Sup. Pisa (4) **30** (2001), no. 1, 225–249.

[3] M. Hata, *Legendre type polynomials and irrationality measures*, J. Reine Angew. Math. **407** (1990), 99–125.

[4] M. Hata, *$\mathbb{C}^2$-saddle method and Beukers' integral*, Trans. Amer. Math. Soc. **352** (2000), no. 10, 4557–4583.

[5] R. Marcovecchio, *The Rhin-Viola method for* $\log 2$, Acta Arith. **139** (2009), 147–184.

[6] R. Marcovecchio and C. Viola, *Irrationality and non-quadraticity measures for logarithms of algebraic numbers*, to appear in J. Australian Math. Soc. .
[7] Yu. V. Nesterenko, *On the irrationality exponent of the number* ln 2 (russian), Mat. Zametki **88** (2010), 549–564; English transl. in Math. Notes **88** (2010), 530–543.
[8] A. A. Polyanskii, *Square exponent of irrationality of* ln 2 (russian), Vestnik Moskov. Univ. Mat. Mekh. **67** (2012), 25–30; English transl. in Mosc. Univ. Math. Bull. **67** (2012), 23–28.
[9] E. A. Rukhadze, *A lower bound for the approximations of* ln 2 *by rational numbers* (russian), Vestnik Moskov. Univ. Ser. I Mat. Mekh. **6** (1987), 25–29,97.
[10] C. Viola, *Hypergeometric functions and irrationality measures*, Analytic number theory (Kyoto, 1996), London Math. Soc. Lecture Note Ser. **247**, 353–360, Cambridge Univ. Press, Cambridge, 1997.

Almost fifth powers in arithmetic progressions

Tünde Kovács
(joint work with Lajos Hajdu)

A celebrated theorem of Erdős and Selfridge [2] states that the product of consecutive positive integers is never a perfect power. A natural generalization is the Diophantine equation

$$x(x+d)\dots(x+(k-1)d) = by^n \tag{1}$$

in non-zero integers x, d, k, b, y, n with $\gcd(x, d) = 1$, $d \geq 1$, $k \geq 3$, $n \geq 2$ and $P(b) \leq k$. Here $P(u)$ stands for the largest prime divisor of a non-zero integer u, with the convention $P(\pm 1) = 1$.

By a conjecture of Erdős, equation (1) has no solutions in positive integers when $k > 3$ and $b = 1$. In other words, the product of k consecutive terms of a primitive positive arithmetic progression with $k > 3$ is never a perfect power. The conjecture of Erdős has recently been verified for certain values of k in a more general form; see the papers [3], [4], [1], [5].

To explain why the case $n = 5$ in equation (1) is special, we need to give some insight into the method of solving (1) for fixed k, in the general case $n \geq 2$. One of the most important tools is the modular method, developed by Wiles. However, the modular technique works effectively only for "large" exponents, typically for $n \geq 7$. Thus the "small" exponents $n = 2, 3, 5$ must be handled separately. In fact these cases are considered in distinct sections, or are covered by separate theorems in the above mentioned papers. Further, the exponents $n = 2, 3$ has already been considered in separate papers. For $n = 2$ and positive x, equation (1) has been completely solved (up to a few exceptional cases) by Hirata-Kohno, Laishram, Shorey and Tijdeman [8] for $k \leq 100$, and in case of $b = 1$, even for $k \leq 109$. Their main tools were elliptic curves and quadratic residues. Later, the exceptional remaining cases have been handled by Tengely [9], by the help of the Chabauty method. When $n = 3$, working mainly with cubic residues, however making use of elliptic curves and the Chabauty method as well, Hajdu, Tengely and Tijdeman [7] obtained all solutions to equation (1) with $k < 32$ such that $P(b) \leq k$ if $4 \leq k \leq 12$ and $P(b) < k$ if $k = 3$ or $k \geq 13$. Further, if $b = 1$ then they could solve (1) for $k < 39$. The case $n = 5$ has not yet been closely investigated. In this case (in the above mentioned papers considering equation (1) for general exponent n) mainly classical methods were used, due to Dirichlet and Lebesgue. Apparently, for $n = 5$ elliptic curves are not applicable. In [6] together with Lajos Hajdu we show that in this case the Chabauty method (both the classical and the elliptic version) can be applied very efficiently. As we mentioned, the Chabauty method has been already used for the cases $n = 2, 3$ in [1], [9], [7]. However, it has been applied only for some particular cases and equations. In our results we solve a large number of genus 2 equations by the Chabauty method, and then build a kind of sieve system based upon them. The theorems that are proved in our paper are the following ones.

Theorem 1. *The product of k consecutive non-zero terms in a primitive arithmetic progression with $3 \le k \le 54$ is never a fifth power.*

Theorem 2. *Equation* (1) *with $n = 5$, $3 \le k \le 24$ and $P(b) \le P_k$ has only "small" solutions (that can be listed explicitly) where the values of P_k are given by*

k	3	4	5	6	7, 8
P_k	3	5	7	11	13
k	9, 10, 11, 12	13, 14, 15	16, 17	18, 19, 20, 21, 22, 23	24
P_k	17	19	23	29	31

As a simple and immediate corollary of Theorem 2 we get the following statement, concerning the case $P(b) \le k$. We mention that already this result yields considerable improvement, in particular with respect to the bound for $P(b)$.

Corollary 1. *For $n = 5$ and $3 \le k \le 36$ all nontrivial solutions of equation* (1) *with $P(b) \le k$ are given by*

$$(k, d) = (3, 7),\ x \in \{-16, -8, -6, 2\};$$
$$(k, d) = (5, 7),\ x \in \{-16, -12\}.$$

Theorem 3. *Let $4 \le t \le 8$ and $z_0 < z_1 < \ldots < z_{t-1}$ be a non-trivial primitive arithmetic progression. Suppose that*

$$z_0 = b_0 x_0^5, z_{i_1} = b_{i_1} x_{i_1}^5, z_{i_2} = b_{i_2} x_{i_2}^5, z_{t-1} = b_{t-1} x_{t-1}^5,$$

with some indices $0 < i_1 < i_2 < t-1$ such that $P(b_0 b_{i_1} b_{i_2} b_{t-1}) \le 5$. Then the initial term z_0 and common difference $z_1 - z_0$ of the arithmetic progression $z_0, \ldots, z_{t-1}$ for the separate values of $t = 4, \ldots, 8$ are "small" and can be listed explicitly.

References

[1] M. A Bennett, N. Bruin, K. Győry and L. Hajdu, *Powers from products of consecutive terms in arithmetic progression*, Proc. London Math. Soc. **92** (2006), 273–306.

[2] P. Erdős and J. L. Selfridge, *The product of consecutive integers is never a power*, Illinois J. Math. **19** (1975), 292–301.

[3] K. Győry, *Power values of products of consecutive integers and binomial coefficients*, Number Theory and Its Applications, Kluwer Acad. Publ. 1999, 145–156.

[4] K. Győry, L. Hajdu and N. Saradha, *On the Diophantine equation $n(n+d)\dots(n+(k-1)d) = by^l$*, Canad. Math. Bull. **47** (2004), 373–388. Correction: Canad. Math. Bull. **48** (2005), 636.
[5] K. Győry, L. Hajdu and Á. Pintér, *Perfect powers from products of consecutive terms in arithmetic progression*, Compositio Math. **145** (2009), 845–864.
[6] L. Hajdu, T. Kovács, *Almost fifth powers in arithmetic progression*, J. Number Theory **131** (2011), 1912–1923.
[7] L. Hajdu, Sz. Tengely and R. Tijdeman, *Cubes in products of terms in arithmetic progression*, Publ. Math. Debrecen **74** (2009), 215–232.
[8] N. Hirata-Kohno, S. Laishram, T. Shorey and R. Tijdeman, *An extension of a theorem of Euler*, Acta Arith. **129** (2007), 71–102.
[9] Sz. Tengely, *Note on the paper "An extension of a theorem of Euler" by Hirata-Kohno et al.*, Acta Arith. **134** (2008), 329–335.

Badly approximable points on a plane and generalized Cantor sets

Dzmitry A. Badziahin

In the talk we consider the sets of badly approximable points on the plane:

$$\mathbf{Bad}(i,j) := \{(\alpha,\beta)\in\mathbb{R}^2 \mid \liminf_{q\to\infty} q\cdot\max\{||q\alpha||^{1/i}, ||q\beta||^{1/j}\} > 0\}$$

where $i,j\ge 0, i+j=1$. One can look at them as the sets of points which coordinates are approximated by rationals in the worst possible way. The parameters i and j reflect the fact that different coordinates are approximated with different speed.

The sets $\mathbf{Bad}(i,j)$ have quite complicated structure. In the talk we present known results about it.

1. The "size" of $\mathbf{Bad}(i,j)$. We can describe it in terms of Lebesgues measure and more deeply in terms of Hausdorff dimension. It is described by the following classical theorems.

Theorem. *For each pair $i,j\ge 0, i+j=1$, $|\mathbf{Bad}(i,j)|=0$ where $|X|$ denotes the Lebesgue's measure of X.*

Theorem (Pollington, Velani, [5]**).** *For the same pairs i,j,* $\dim(\mathbf{Bad}(i,j)) = 2 = \mathrm{FULL}$ *where* $\dim(X)$ *denotes the Hausdorff dimension of X.*

Thus shows that sets $\mathbf{Bad}(i,j)$ are quite small but not too much small.

2. Relation between sets. There is no straightforward relation between sets $\mathbf{Bad}(i,j)$ for different pairs (i,j). In particular it was not even known until recently that any two of them have nonempty intersection. This problem was firstly posed by Schmidt in 1980's in the following way:

Problem (Schmidt). *The set* $\mathbf{Bad}(1/3,2/3)\cap\mathbf{Bad}(2/3,1/3)$ *is nonempty.*

Later this problem was generalised for an arbitrary pair of parameters (i_1,j_1) and (i_2,j_2). It remained open until 2010 when it was proven in full by D., Pollington and Velani [1]:

Theorem (D., Pollington, Velani). *Let (i_t,j_t) be a countable number of pairs of real numbers satisfying $i_t,j_t\ge 0, i_t+j_t=1$ and let* $i := \sup\{i_t : t\in\mathbb{N}\}$. *Suppose* *that*

$$\liminf_{t\to\infty} \min\{i_t, j_t\} > 0 \ . \tag{1}$$

Then, for any $\theta \in \mathbf{Bad}(i)$ *we have that*

$$\dim\Big(\bigcap_{t=1}^{\infty} \mathbf{Bad}(i_t, j_t) \cap L_\theta\Big) = 1 \ .$$

Later in 2012 J. An by developing the ideas of the paper managed to remove the technical condition (1).

It is worth mentioning that Schmidt's problem is closely related to another famous conjecture in Diophantine approximation posed by Littlewood:

Conjecture (Littlewood). *For each point* $(x, y) \in \mathbb{R}^2$

$$\liminf_{q\to\infty} q||q\alpha|| \cdot ||q\beta|| = 0$$

where $||x||$ *means the distance to the nearest integer.*

One can check that any potential counterexample to Littlewood conjecture must be in every set $\mathbf{Bad}(i, j)$. Therefore if someone could find the intersection of $\mathbf{Bad}(i, j)$ which is empty it would have proven the conjecture.

3. The structure of $\mathbf{Bad}(i, j)$ on planar curves. The first problem in this direction was posed by Davenport in 1960's [4].

Problem (Davenport). *there are uncountably many points from* $\mathbf{Bad}(1/2, 1/2)$ *on the parabola* (x, x^2).

One countable family of such points on a parabola can be achieved from of Cassels and Swinnerton-Dyer [3]. They showed that if $1, \alpha, \beta$ are linearly independent elements from the same cubic field then $(\alpha, \beta) \in \mathbf{Bad}(1/2, 1/2)$.

In full generality Davenport problem was proven in 2012 by D. and Velani [2]

Theorem (D., Velani). *Let* $\mathcal{C}$ *be two time continuously differentiable curve such that its curvature is non-zero at least in one point. Then*

$$\dim(\mathbf{Bad}(i, j) \cap \mathcal{C}) = 1 = \text{FULL}.$$

If $\mathcal{C}$ is a straight line that the result is not true in general. One can find such a line $\mathcal{L}$ that the intersection $\mathbf{Bad}(i, j) \cap \mathcal{L}$ is empty. However it can be proven for lines $\mathcal{L}$ with some additional conditions on their coefficients:

Theorem (D., Velani). *Let* $\mathcal{L} : y = \alpha x + \gamma$ *be a line such that* $\exists \epsilon > 0$ *which satisfies*

$$\liminf_{q\to\infty} q^{\max\{1/i, 1/j\}-\epsilon}||q\alpha|| > 0.$$

Then

$$\dim(\mathbf{Bad}(i, j) \cap \mathcal{C}) = 1 = \text{FULL}.$$

4. Winning property. Recently J. An managed to prove that the set $\mathbf{Bad}(i, j)$ is α winning for some positive number α. This quite powerful property of the sets was firstly introduced by Schmidt [6]. In particular winning sets have the full Hausdorff dimension and a countable intersection of winning sets is again winning.

All the mentioned results of the speaker and Velani are achieved with help of generalised Cantor-type sets. They are constructed similarly to the middle-third Cantor set but in much more general way. It appears that they satisfy some very nice properties. Firstly one can estimate their Hausdorff dimension (especially its lower bound). And the intersection of two Cantor-type sets can often be considered as another Cantor-type set which helps to estimate the "size" of their intersection. For more information on generalized Cantor sets see [2].

References

[1] D. Badziahin, A. Pollington, S. Velani *On a problem in simultaneous Diophantine approximation: Schmidt's conjecture*, Annals of Math. **174** (2011), 1837–1883.

[2] D. Badziahin, S. Velani *Multiplicatively badly approximable numbers and generalized Cantor sets*, Advances in Math., **228(5)** (2011), 2766–2796.

[3] J.W.S. Cassels, H.P.F. Swinnerton-Dyer *On the product of three homogeneous linear forms and the indefinite ternary quadratic forms.*, Philos. Trans. Roy. Soc. London, **248** (1955), 73–96.

[4] H. Davenport *A note on Diophantine approximation. II*, Mathematika, **11** (1964), 50–58.

[5] A. Pollington, S. Velani *On a problem in simultaneously Diophantine approximation: Littlewood's conjecture*, Acta Math. **66** (2000), 29–40.

[6] W. Schmidt *Diophantine approximation*, Lecture notes in mathematics, 785 Springer, Berlin. (1980).

A generalization of Schanuel's Theorem

Martin Widmer

(joint work with Christopher Frei)

Let k be a number field, let θ be a nonzero algebraic number, let $H(\cdot)$ denote the usual multiplicative absolute Weil height on the algebraic numbers, and write $N(\theta k, X)$ for the number of $\alpha \in k$ with $H(\theta\alpha) \leq X$. For $\theta = 1$ (or what is the same for $\theta \in k$) the quantity $N(\theta k, X)$ is fairly well understood. For instance, a classical result due to Schanuel [3] gives the asymptotics

$$N(k, X) = S_k X^{2d} + O(X^{2d-1} \log X),$$

as X tends to infinity. Here d is the degree of k, and S_k is defined as

$$S_k = \frac{h_k R_k}{w_k \zeta_k(2)} \left(\frac{2^{r_k} (2\pi)^{s_k}}{\sqrt{|\Delta_k|}} \right)^2 2^{r_k + s_k - 1},$$

where h_k is the class number, R_k the regulator, w_k the number of roots of unity in k, ζ_k the Dedekind zeta-function of k, Δ_k the discriminant, r_k is the number of real embeddings of k, and s_k is the number of pairs of distinct complex conjugate embeddings of k.

Evertse was the first to consider the general quantity $N(\theta k, X)$. The proof of his celebrated uniform upper bounds [1] for the solutions of S-unit equations over

k involves a uniform upper bound for $N(\theta k, X)$. The latter was refined by Schmidt [4], and further improved by Loher and Masser [2], who showed

$$N(\theta k, X) \leq 68(d \log d) X^{2d}, \tag{1}$$

provided $d > 1$, and $N(\theta\mathbb{Q}, X) \leq 17X^2$.

All the proofs of these upper bounds rely in an essential way on the box-principle which works well for upper bounds but seems inappropriate to produce asymptotic results. This may have motivated Loher and Masser's following statement [2, p.279] regarding their bound on $N(\theta k, X)$:"*It would be interesting to know if there are asymptotic formulae like Schanuel's for the cardinalities here, at least for fixed θ not in k.*" Our first theorem responds to this problem. But first we require to introduce some notation.

Let $K = k(\theta)$. For each Archimedean place v of k (or w of K) we choose the unique absolute value $|\cdot|_v$ on k (or $|\cdot|_w$ on K) that extends the usual Euclidean absolute value on $\mathbb{Q}$. We also fix a completion k_v of k at v, and we define a set of points $(z_0, z_1) \in k_v^2$ by

$$\prod_{w|v} \max\{|\theta|_w |z_0|_v, |z_1|_v\}^{[K_w:k_v]} < 1,$$

where the product runs over all places w of K extending the Archimedean place v of k. These sets are measurable and have a finite volume which we denote by V_v. We put

$$V = V(\theta, k) = (2^{r_k}\pi^{s_k})^{-2} \prod_{v|\infty} V_v.$$

Let μ_k be the Möbius function on k, and write $\mathcal{O}_k$ for the ring of integers of k. For a fractional ideal B of k let ${}^uB$ be the smallest fractional ideal of K containing B. Finally, we use $\mathfrak{N}_k(\cdot)$ for the norm map on the fractional ideals of k.

Note that $N(\theta k, X) = N(\alpha\theta k, X)$ for any nonzero $\alpha \in k$. Thus without loss of generality we may and will assume θ be integral. Let $\mathfrak{D} = \theta\mathcal{O}_K$, and $D = \mathfrak{D} \cap \mathcal{O}_k$. We define

$$g_k(\theta) = V \sum_{B|D} \frac{\mathfrak{N}_K(\mathfrak{D}, {}^uB)^{\frac{2}{[K:k]}}}{\mathfrak{N}_k B} \sum_{A|B^{-1}D} \frac{\mu_k(A)}{\mathfrak{N}_k A} \prod_{P|AB} \frac{\mathfrak{N}_k P}{\mathfrak{N}_k P + 1}. \tag{2}$$

Theorem 1. *Let θ be a nonzero algebraic integer, let k be a number field and denote its degree by d. Then, as $X \geq 1$ tends to infinity, we have*

$$N(\theta k, X) = g_k(\theta) S_k X^{2d} + O(X^{2d-1}\mathfrak{L}),$$

where $\mathfrak{L} = \log(X+1)$ if $d = 1$ and $\mathfrak{L} = 1$ otherwise. The implicit constant in the O-term depends on θ and on k.

The standard inequalities $H(\alpha)/H(\theta) \leq H(\alpha\theta) \leq H(\alpha)H(\theta)$, combined with Schanuel's result, imply

$$H(\theta)^{-2d} \leq g_k(\theta) \leq H(\theta)^{2d}.$$

One then may ask if there are uniform (in k or in θ or even in k and θ) lower and upper bounds for $g_k(\theta)$. For the lower bound we consider the example $\theta = \sqrt{p}$ with p a rational prime, inert in k. Then from (2) we get

$$g_k(\theta) = g_k(\sqrt{p}) = \frac{2p^{d/2}}{p^d + 1}.$$

Fixing k and letting p tend to infinity we see that there is no lower bound for $g_k(\theta)$ that is uniform in θ. Likewise, fixing p and letting d tend to infinity shows that there is no lower bound, uniform in d.

On the other hand, from (1) we conclude (for $d > 1$)

$$g_k(\theta) \leq \frac{68d \log d}{S_k},$$

and thus there is also an upper bound that is uniform in θ. But for fixed θ one would expect that for "most" $\alpha \in k$ one has $H(\alpha\theta) \geq H(\alpha)$, and thus one might even conjecture $g_k(\theta) \leq 1$. Indeed, using a more appropriate representation of $g_k(\theta)$ as an Euler-product we have shown that this "conjecture" holds true.

Theorem 2. *We have*

$$g_k(\theta) \leq 1.$$

References

[1] J. H. Evertse, *On equations in S-units and the Thue-Mahler equation*, Invent. Math. **75** (1984), 561–584.

[2] T. Loher and D. W. Masser, *Uniformly counting points of bounded height*, Acta Arith. **111** (2004), 277–297.

[3] S. H. Schanuel, *Heights in number fields*, Bull. Soc. Math. France **107** (1979), 433–449.

[4] W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Lecture Notes in Mathematics 1467, Springer, 1991.

Exceptional units and cyclic resultants

Cameron L. Stewart

Let α be a non-zero algebraic integer of degree d over $\mathbb{Q}$. Put $K = \mathbb{Q}(\alpha)$ and let $\mathcal{O}_K$ denote the ring of algebraic integers of K. Let $E(\alpha)$ be the number of positive integers n for which $\alpha^n - 1$ is a unit in $\mathcal{O}_K$. If $\alpha - 1$ is not a unit define $E_0(\alpha)$ to be 0 and otherwise define $E_0(\alpha)$ to be the largest integer n such that $\alpha^j - 1$ is a unit for $1 \leq j \leq n$. Let $\Phi_n(x)$ be the n-th cyclotomic polynomial. Define $U(\alpha)$ to be the number of positive integers n for which $\Phi_n(\alpha)$ is a unit.

We discussed estimates for $E_0(\alpha)$, $E(\alpha)$ and $U(\alpha)$. Certainly $E_0(\alpha) \leq E(\alpha) \leq U(\alpha)$. We have, for example, that there is an effectively computable positive number c such that if α is a non-zero algebraic integer of degree d over the rationals then

$$E_0(\alpha) < cd\frac{(\log(d+1))^4}{(\log\log(d+2))^3}.$$

For any positive integer d let us define $e(d)$ by $e(d) = \max\{E_0(\alpha) | \alpha$ an algebraic integer of degree $d\}$. We showed that $e(d) = d$ for $d = 1, \ldots, 6, e(7) < 7$ and $e(8) \geq 7$. We conjectured that $e(d) < d$ for $d \geq 7$.

Greatest Common Divisors of $u - 1, v - 1$ in positive characteristic and rational points on curves over finite fields

Pietro Corvaja
(joint work with Umberto Zannier)

This is a report on a joint work with U. Zannier which will be published on the Journal of the European Mathematical Society.

In the work [2] an upper bound was proved for the $\gcd(u-1, v-1)$, for S-units u, v of a function field in characteristic zero. Namely, we proved

Theorem 1. *Let κ be an algebraically closed field of characteristic zero, X be a smooth projective curve over κ, $u, v \in \kappa(X)$ non-constant multiplicatively independent rational functions, $S \subset X(\kappa)$ its set of zeros and poles. Then*

$$\sum_{\nu \in X(\kappa) \setminus S} \min\{\nu(1-u), \nu(1-v)\} \leq 3\sqrt[3]{2}(\deg(u)\deg(v)\chi)^{1/3}. \tag{1}$$

In the above inequality, as in the sequel, ν also stands for the valuation canonically associated to the point ν of a curve. The left-hand side is the function field analogue of the (logarithmic) Greatest Common Divisor of the regular functions $u - 1, v - 1$.

This generalized an analogous bound holding over number fields, proved in [1]. As pointed out by Silverman [5], the exact analogue does not work for function fields in positive characteristic. Actually, if an affine curve is given by an equation of the form $f(x, y) = 0$ over the finite field $\mathbb{F}_q$, then letting $u = x^{q^n - 1}, v = y^{q^n - 1}$ it turns out that the left-hand side above is at least the number of q^n-rational points on the curve. Hence, by Weil's estimates, it tends to infinity asymptotically as q^n, which, up to a constant, is the degree of u and v.

I shall present a possible extension in the direction of positive characteristic; it turns out that under suitable assumptions some of the results still hold. For instance we proved Theorems 2 and 3 below, from which we deduce in particular a new proof of Weil's bound for the number of rational points on a curve over finite fields. When the genus of the curve is large compared to the characteristic, we can even go beyond it.

What seems a new feature is the analogy with the characteristic zero case, which admitted applications to apparently distant problems.

Theorem 2. *Let X be a smooth projective absolutely irreducible curve over a field κ of characteristic p. Let $u, v \in \kappa(X)$ be rational functions, multiplicatively* *independent modulo κ^*, and with non-zero differentials; let S be the set of their zeros and poles, $\chi = |S| + 2g - 2$ be the Euler characteristic of $X \setminus S$. Then*

$$\sum_{\nu \in X(\overline{\kappa}) \setminus S} \min\{\nu(1-u), \nu(1-v)\} \le \max\left(3\sqrt[3]{2}(\deg u \deg v\, \chi)^{1/3},\, 12\frac{\deg u \deg v}{p}\right).$$

Observe that we recover the same bound of Theorem 1 when

$$32(\deg u \deg v)^2 \le p^3 \chi.$$

The above theorem admits the following corollary, which can also be deduced by recent work of Heath-Brown and Konyagin [4]

Corollary 1. *Let $X \subset \mathbf{G}_m^2$ be an absolutely irreducible plane curve of Euler characteristic χ, not the translate of a subtorus. Suppose it is defined by an equation $f(x, y) = 0$ of bidegree (d_1, d_2). Denote by μ_m the group of m-th roots of unity in $\mathbb{F}_{\shortparallel}{}^*$.*

Then

$$|X \cap (\mu_{m_1} \times \mu_{m_2})| \le \max\left(3\sqrt[3]{2}(m_1 m_2 d_1 d_2 \chi)^{1/3}, 12\frac{m_1 m_2 d_1 d_2}{p}\right).$$

The following general result enables us to deduce an estimate for the number of rational points over $\mathbb{F}_{q^2}$ of a curve defined over $\mathbb{F}_q$ which turns out to be sufficient to recover Weil's theorem:

Theorem 3. *Let $\kappa \subset \mathbb{F}_q$, L be a 1-dimensional function field over κ. Let x, y be separating elements in L. Let $f(x, y) = 0$ be the minimal relation between x and y, with coefficient in κ, where $f(X, Y) \in \kappa[X, Y]$ is supposed to be absolutely irreducible. Let C be a smooth projective model of the function field L and let $S \subset C$ be a finite set containing all the zeros and poles of x, y; we denote by χ the Euler characteristic of $C \setminus S$. Let $a = \deg_X f, b = \deg_Y f$.*

Let h, k be positive integers with

$$ah + bk < q. \tag{2}$$

Put $u = xz^q, v = yw^q$ for some S-units $z, w \in L^*$. Then at least one of the two alternatives holds:

(1) $a \le k$ and $b \le h$,

or

(2) $\sum_{\nu \notin S} \min\{\nu(1-u), \nu(1-v)\} \le \frac{q+k-hk}{q}\deg(v) + \frac{k}{q}\deg(u) + \frac{q-1}{2}\chi$.

To deduce an upper bound for the number of $\mathbb{F}_{q^2}$-rational points just take $z = x^{-q}, w = y^{-q}$. Then u, v take the value 1 precisely on the $\mathbb{F}_{q^2}$-rational points. From this fact we deduce a best-possible (up to a constant) upper bound for the number of rational points over any finite field of type $\mathbb{F}_{q^{2n}}$. It is well known that this implies Weil's theorem (i.e. Riemann hypothesis for the field L over $\mathbb{F}_q$).

While our proof in [2] used Wronskian, in the positive characteristic case we are forced to use the so-called hyper-Wronskian, associated to the hyper-derivative operators, as in works of Garcia and Voloch [3].

References

[1] P. Corvaja, U. Zannier, A lower bound for the height of a rational function at S-unit points, *Monatshefte für Math.* **144** (2005), 203-224.

[2] P. Corvaja, U. Zannier, Some cases of Vojta's conjecture on integral points over function fields, *Journal Alg. Geometry* **17** (2008), 295-333. *Addendum* in *Asian Journal of Math.* **14**, 4, 581-584 (2010).

[3] A. Garcia, J.F. Voloch, Wronskians and linear independence in fields of prime characteristic, *Manuscripta Math.* **59**, 457-469 (1987).

[4] D.R. Heath-Brown, S. Konyagin, New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum, *Q. J. Math.* **51** (2000), 221–235.

[5] J. Silverman, Common divisors of $a^n - 1$ and $b^n - 1$ over function fields, *New York J. Math.* **10** (2004), 37-43.

Simultaneous approximation with polynomials and their derivatives

Victor Beresnevich

(joint work with G. A. Margulis)

Let $n \in \mathbb{N}$. Given a polynomial $P(x) = a_n x^n + \cdots + a_0$ with integer coefficients, let $H(P) = \max_{0\le i\le n} |a_i|$ denote the height of P. It is a well known consequence of Minkowski's theorem that for every $x \in \mathbb{R}$ with $|x| \le 1/2$ there are infinitely many $P \in \mathbb{Z}[x]$ with $\deg P \le n$ such that $|P(x)| < H(P)^{-n}$. Motivated by a classification of transcendental numbers, in 1932 Mahler [12] conjectured that for any $\varepsilon > 0$ for almost all real x there are only finitely many $P \in \mathbb{Z}[x]$ with $\deg P \le n$ such that

$$|P(x)| < H(P)^{-n-\varepsilon}\,.$$

Mahler himself proved such a statement with $\varepsilon > 3n$. Various partial results were obtained over a period of 30 years and the conjecture was eventually established by Sprindžuk in 1965 – see [13] for a full account. Subsequent developments include Diophantine approximation on manifolds and the Khintchine-Groshev type results see [1, 2, 7, 8, 9, 10, 11, 14]. The crux of establishing the Khintchine-Groshev type results was the study of systems of Diophantine inequalities that involved both linear forms and their derivatives. The idea was introduced by Bernik [9] in the context of polynomials who proved that for any $n \in \mathbb{N}$ and any $\varepsilon > 0$ for almost all $x \in \mathbb{R}$ there are only finitely many $P\ in\mathbb{Z}[x]$ with $\deg P \le n$ satisfying

$$\text{(1)}\qquad \begin{cases} |P(x)| < H(P)^{-n}, \\ |P'(x)| < H(P)^{1-\varepsilon}. \end{cases}$$

Indeed, while establishing Khintchine-Groshev type results, eliminating instances of approximation with small derivatives such as in (1) leads to a linearizable problem that is generally deal with much easier.

In recent years, there has also been a growing interest in results that involve more general systems of inequalities that include derivatives of higher orders. In particular, the motivation comes from the study of rational points near manifolds [3], close conjugate algebraic pairs [5] and the distribution of discriminants and resultants [4, 6].

The following general results regarding systems of linear forms that involve all the derivatives of a polynomial of degree n have been recently obtained in collaboration with Margulis.

Theorem 1. *Let $n \in \mathbb{N}$ and $\varepsilon > 0$. Then, for almost all $x \in \mathbb{R}$ there are only finitely many $P \in \mathbb{Z}[x]$ with $\deg P = n$ such that*

$$\prod_{i=0}^{n} |P^{(i)}(x)| < H(P)^{-\varepsilon} . \tag{2}$$

The condition on ε is clearly optimal. This theorem can also be restated in the following equivalent form.

Theorem 1′. *Let $n \in \mathbb{N}$ and $v_0, \dots, v_n \in \mathbb{R}$ satisfy $v_0 + \cdots + v_n > 0$. Then, for almost all $x \in \mathbb{R}$ there are only finitely many $P \in \mathbb{Z}[x]$ with $\deg P = n$ satisfying*

$$|P^{(i)}(x)| < H(P)^{-v_i} \qquad (0 \le i \le n) . \tag{3}$$

Mahler's conjecture essentially corresponds to the case $v_1 = \cdots = v_n = -1$. The case $v_2 = \cdots = v_n = -1$ is proved in [8, §8.3]. Yet another case when $v_0, \dots, v_{m-1} \ge 0$ and $v_m, \dots, v_n \le 0$ for some m, was considered in [5, Theorem 4].

Theorem 1 is deduced from the following effective result.

Theorem 2. *Let $n \ge 1$, $J \subset \mathbb{R}$ be any interval of length 1, $\theta_0, \dots, \theta_n > 0$ and*

$$A_n^*(J; \theta_0, \dots, \theta_n) = \left\{ x \in J : \begin{array}{l} \exists\ P \in \mathbb{Z}[x] \setminus \{0\} \text{ such that } \deg P = n \text{ and} \\ |P^{(i)}(x)| \le \theta_i \quad \text{for all } i \in \{0, \dots, n\} \end{array} \right\} .$$

Then

$$\lambda\big(A_n^*(J; \theta_0, \dots, \theta_n)\big) \le 6^n (n+1)^5 \left(\theta_0 \dots \theta_n\right)^{4(n+1)^{-3}},$$

where λ denotes Lebesgue measure in $\mathbb{R}$.

The term $H(P)^{-\varepsilon}$ can be replaced with $\big(\log H(P)\big)^{-\frac{1}{4}(n+1)^3 - \varepsilon}$. Other more general forms of Theorems 1 and 2 obtained involve results for lacunary polynomials. The proofs make use of a theorem of Kleinbock and Margulis [11] and the calculous of binomial determinants.

References

[1] V. Beresnevich, *On approximation of real numbers by real algebraic numbers.* Acta Arith. **90** (1999), 97–112.

[2] V. Beresnevich, *A Groshev type theorem for convergence on manifolds.* Acta Math. Hungar. **94** (2002), 99–130.

[3] V. Beresnevich, *Rational points near manifolds and metric Diophantine approximation.* Ann. of Math. (2) **175** (2012), 187–235.

[4] V. Beresnevich, V. Bernik, and F. Götse, *On the distribution of the values of the resultants of integral polynomials.* Dokl. Nats. Akad. Nauk Belarusi **54** (2010), no. 5, 21–23.

[5] V. Beresnevich, V. Bernik, and F. Götze, *The distribution of close conjugate algebraic numbers.* Compos. Math. **146** (2010), no. 5, 1165–1179.

[6] V. Beresnevich, V. Bernik, and F. Götze, *Simultaneous approximations of zero by an integral polynomial, its derivative, and small values of discriminants.* Dokl. Nats. Akad. Nauk Belarusi **54** (2010), no. 2, 26–28.
[7] V. Beresnevich, V. I. Bernik, D. Y. Kleinbock, and G. A. Margulis, *Metric Diophantine approximation: the Khintchine-Groshev theorem for nondegenerate manifolds.* Mosc. Math. J. **2** (2002), no. 2, 203–225.
[8] V. Bernik, D. Kleinbock, and G. A. Margulis, *Khintchine-type theorems on manifolds: the convergence case for standard and multiplicative versions.* Internat. Math. Res. Notices, **2001** (2001), no. 9, 453–486.
[9] V. I. Bernik, *On the exact order of approximation of zero by values of integral polynomials.* Acta Arithmetica **53** (1989), 17–28. (In Russian).
[10] D. Kleinbock, G. Margulis, and J. Wang, *Metric Diophantine approximation for systems of linear forms via dynamics.* Int. J. Number Theory, **6** (2010), no. 5, 1139–1168.
[11] D. Y. Kleinbock and G. A. Margulis, *Flows on homogeneous spaces and Diophantine approximation on manifolds.* Ann. of Math. (2), **148** (1998), 339–360.
[12] K. Mahler, *Über das Maßder Menge aller S-Zahlen.* Math. Ann. **106** (1932), 131–139.
[13] V.G. Sprindžuk, *Mahler's problem in the metric theory of numbers*, Translations of Mathematical Monographs Vol. 25. Amer. Math. Soc., Providence, RI, 1969.
[14] V.G. Sprindžuk, *Metric theory of Diophantine approximation.* John Wiley & Sons, New York-Toronto-London, 1979.

Overdetermined systems of lacunary equations

Francesco Amoroso
(joint work with Louis Leroux, Martín Sombra)

Let $f,\ g \in \mathbb{Z}[x]$ be polynomials of degree $\le d$, of bounded height and having a bounded number of non zero coefficients. Assuming that at least one of f and g does not vanish at any roots of unity, Filaseta, Granville and Schinzel [2] proved that there exists an algorithm which computes the greatest common divisor of f and g in $O(\log d)$ arithmetic operations.

This result heavily relies on a work of Bombieri and Zannier on the intersection of a subvariety of $\mathbb{G}_{\mathrm{m}}^n$ of codimension ≥ 2 with subgroups of dimension 1. This work appeared for the first time as an appendix of a book of Schinzel [3] by Zannier and later, in a refined form, in a joint paper of Bombieri, Masser and Zannier [1]. It is a special case of the following open conjecture of Zilber.

Conjecture 1. *Let W be an algebraic subset of $\mathbb{G}_{\mathrm{m}}^N$. Then there exists a finite collection $\mathcal{U}_W$ of codimension 1 torsion cosets (= translates of subtori by torsion points) of $\mathbb{G}_{\mathrm{m}}^N$ satisfying the following property. Let $T_0 \subset \mathbb{G}_{\mathrm{m}}^N$ be a torsion coset and let Y be an irreducible component of $\overline{W} \cap T_0$ of dimension*

$$\dim Y > \dim W - \operatorname{codim} T_0\ .$$

Then there exists $T \in \mathcal{U}_W$ such that $Y \subseteq W \cap T$.

Assuming this conjecture, we generalize the result of Filaseta-Granville-Schinzel to overdetermined systems of lacunary equations.

Theorem 2. *Let us assume Zilber conjecture. Let $V \subset \mathbb{G}_{\rm m}^n$ be a subvariety defined over a number field K by a bounded number of equations of degree $\leq d$ of bounded height and supported by a bounded number of monomials. Then we can find in at most*

$$O(\log d)$$

arithmetic operations a finite collection Γ whose elements are sequences

$$(P_1, \ldots, P_L, Q) \qquad \text{with} \qquad L \leq n$$

of Laurent polynomials, such that

$$V = \bigcup_{\Gamma} (Z(P_1, \ldots, P_L) \backslash Z(Q)) \, .$$

Moreover, every irreducible component

$$X \subseteq \overline{Z(P_1, \ldots, P_L) \backslash Z(Q)}$$

has codimension L.

References

[1] E. Bombieri, D. Masser and U. Zannier, *Anomalous subvarieties-structure theorems and applications.* IMRN 2007, no. 19, 33p.

[2] M. Filaseta, A. Granville and A. Schinzel, *Irreducibility and greatest common divisor algorithms for sparse polynomials. In Number theory and polynomials*, 155–176, London Math. Soc. Lecture Note Ser., **352**, Cambridge Univ. Press, Cambridge, 2008.

[3] A. Schinzel, *Polynomials with special regard to reducibility.* With an appendix by Umberto Zannier. Encyclopedia of Mathematics and its Applications, **77**. Cambridge University Press, Cambridge, 2000.

Diagonalization and rationalization

Boris Adamczewski

(joint work with Jason P. Bell)

Given a field K and a multivariate power series

$$f(x_1, \ldots, x_n) := \sum_{(i_1, \ldots, i_n) \in \mathbb{N}^n} a(i_1, \ldots, i_n) x_1^{i_1} \cdots x_n^{i_n}$$

with coefficients in K, we define the *diagonal* $\Delta(f)$ of f as the one variable power series

$$\Delta(f)(t) := \sum_{n=0}^{+\infty} a(n, \ldots, n) t^n \in K[[t]] \, .$$

In the case where $K = \mathbb{C}$, diagonalization may be nicely visualized thanks to Deligne's formula via contour integration over a vanishing cycle. Formalizing this in terms of the Gauss–Manin connection and De Rham cohomology groups, and using a deep result of Grothendieck, one can prove that the diagonal of any algebraic power series with algebraic coefficients is a Siegel G-function that comes from geometry, that is, one which satisfies the Picard–Fuchs type equation associated with some one-parameter family of algebraic varieties. As claimed by the Bombieri–Dwork conjecture, this is a picture expected for all G-functions. Diagonals of algebraic power series with coefficients in $\overline{\mathbb{Q}}$ thus appear to be a distinguished class of G-functions.

When K is a field of positive characteristic, the situation is completely different as shown the following nice result due to Furstenberg and Deligne: the diagonal of an algebraic power series in $K[[x_1,\dots,x_n]]$ is algebraic. Given a prime number p and a power series $f(x) := \sum_{n=0}^{+\infty} a(n)x^n \in \mathbb{Z}[[x]]$, we denote by $f_{|p}$ the reduction of f modulo p, that is

$$f_{|p}(x) := \sum_{n=0}^{+\infty} (a(n) \bmod p)x^n \in \mathbb{F}_p[[x]]\,.$$

The Furstenberg–Deligne theorem implies that if $f(x_1,\dots,x_n) \in \mathbb{Z}[[x_1,\dots,x_n]]$ is algebraic over $\mathbb{Q}(x_1,\dots,x_n)$, then $\Delta(f)_{|p}$ is algebraic over $\mathbb{F}_p(t)$ for every prime p. It now becomes very natural to ask how the complexity of the algebraic function $\Delta(f)_{|p}$ may increase when p run along the primes. Deligne obtained a first result in this direction by proving that if $f(x,y) \in \mathbb{Z}[[x,y]]$ is algebraic, then, for all but finitely many primes p, $\Delta(f)_{|p}$ is an algebraic power series of degree at most Ap^B, where A and B do not depend on p but only on explicit geometric quantities associated with f. He also suggested that a similar bound should hold for the diagonal of algebraic power series in $\mathbb{Z}[[x_1,\dots,x_n]]$. In this talk, I will discuss the following answer to the question raised by Deligne.

Theorem. Let $f(x_1,\dots,x_n) \in \mathbb{Z}[[x_1,\dots,x_n]]$ be an algebraic power series with degree at most d and height at most h. Then there exists an effective constant $A := A(n,d,h)$ depending only on n, d and h, such that $\Delta(f)_{|p}$ has degree at most p^A and height at most A^2p^{A+1}, for every prime number p.

Problems surrounding the mixed Littlewood conjecture for pseudo-absolute values

Stephen Harrap
(joint work with Alan Haynes)

For $x \in \mathbb{R}$ let $\|x\|$ denote the distance from x to the nearest integer. The Littlewood Conjecture is the assertion that for every $x_1, x_2 \in \mathbb{R}$,

$$\inf_{q\in\mathbb{N}} q\,\|qx_1\|\,\|qx_2\| \;=\; 0. \tag{1}$$

This conjecture has come to light recently because of its connection to measure rigidity problems for diagonal actions on the space of unimodular lattices. This connection was exploited by Einsiedler, Katok, and Lindenstrauss [3] to show the set of pairs $(x_1,x_2) \in \mathbb{R}^2$ which do not satisfy (1) has Hausdorff dimension zero.

More recently de Mathan and Teulié [8] have proposed a problem which is closely related to the Littlewood Conjecture. Let $\mathcal{D} = \{n_k\}_{k\geq 0}$ be an increasing sequence of positive integers with $n_0 = 1$ and $n_k|n_{k+1}$ for all k. We refer to such a sequence as a *pseudo-absolute value sequence*, and we define the *$\mathcal{D}$-adic pseudo-absolute value* $|\cdot|_{\mathcal{D}} : \mathbb{N} \to \{n_k^{-1} : k \geq 0\}$ by

$$|q|_{\mathcal{D}} = \min\{n_k^{-1} : q \in n_k\mathbb{Z}\}.$$

In the case when $\mathcal{D} = \{a^k\}_{k=0}^{\infty}$ for some integer $a \geq 2$ we also write $|\cdot|_{\mathcal{D}} = |\cdot|_a$. If p is a prime then $|\cdot|_p$ is the usual $p-$adic absolute value.

The de Mathan and Teulié Conjecture, which we will refer to as the Mixed Littlewood Conjecture, is the assertion that for any $\mathcal{D}$ and for every $x \in \mathbb{R}$,

$$\inf_{q\in\mathbb{N}} q\,|q|_{\mathcal{D}}\,\|qx\| \;=\; 0. \tag{2}$$

By employing connections with measure rigidity results in this setting Einsiedler and Kleinbock [4] proved that when $|\cdot|_{\mathcal{D}} = |\cdot|_a$ the set of $x \in \mathbb{R}$ which do not satisfy (2) has Hausdorff dimension zero.

The case of the Mixed Littlewood Conjecture with more than one pseudo-absolute value has also been a topic of recent interest. If $\mathcal{D}_1$ and $\mathcal{D}_2$ are two pseudo-absolute value sequences it is reasonable to conjecture that for any $x \in \mathbb{R}$,

$$\inf_{q\in\mathbb{N}} q|q|_{\mathcal{D}_1}|q|_{\mathcal{D}_2}\|qx\| = 0. \tag{3}$$

Remarkably, it is shown in [4] that the Furstenberg Orbit Closure Theorem [5, Theorem IV.1] implies that (3) is true whenever $\mathcal{D}_1 = \{a^k\}$ and $\mathcal{D}_2 = \{b^k\}$ for two multiplicatively independent integers a and b. This result was strengthened by Bourgain, Lindenstrauss, Michel, and Venkatesh [1] who proved a result which implies (see [2, Section 4.6]) that there is a constant $\kappa > 0$ such that for all $x \in \mathbb{R}$,

$$\inf_{q\in\mathbb{N}} q(\log\log\log q)^{\kappa}|q|_a|q|_b\|qx\| = 0.$$

Their results provide a contrast to the situation of the original Littlewood Conjecture, where nothing seems to be gained by adding more real variables.

It was pointed out by Einsiedler and Kleinbock in [4] that the dynamical machinery used to study these problems does not readily extend to the case of more general pseudo-absolute values. Our first result demonstrates how recent measure rigidity theorems can be combined with bounds for linear forms in logarithms to obtain more general results.

Theorem 1 ([7]). *Suppose that $a \geq 2$ is an integer and that $\mathcal{D} = \{n_k\}$ is a pseudo-absolute value sequence all of whose elements are divisible by finitely many fixed primes coprime to a. If there is a $\delta \geq 0$ with*

$$\log n_k \leq k^{\delta} \quad \text{for all} \quad k \geq 2, \tag{4}$$

then for any $x \in \mathbb{R}$ we have that

$$\inf_{q\in\mathbb{N}} q|q|_a|q|_{\mathcal{D}}\|qx\| = 0. \tag{5}$$

Of particular interest is the case when consecutive elements of the sequence $\mathcal{D}$ have bounded ratios (cf. [4, 8]), and we will say that $\mathcal{D}$ and $|\cdot|_{\mathcal{D}}$ have bounded ratios in this case. For the bounded ratios case our theorem gives a quite satisfactory answer to the problem at hand.

Corollary 1 ([7]). *Suppose that $a \geq 2$ is an integer and that $\mathcal{D}$ is a pseudo-absolute value sequence with bounded ratios, all of whose elements are coprime to a. Then for any $x \in \mathbb{R}$ we have that*

$$\inf_{q\in\mathbb{N}} q|q|_a|q|_{\mathcal{D}}\|qx\| = 0.$$

After establishing Theorem 1 we turn to the problem of determining the almost everywhere behavior of the quantities on the left hand side of (2). The analogue of this problem for the Littlewood Conjecture was established by Gallagher [6]. He proved that if $\psi : \mathbb{N} \to \mathbb{R}$ is any non-negative decreasing function for which

$$\sum_{r\in\mathbb{N}} \log(r)\psi(r) = \infty \tag{6}$$

then for almost every $(x_1, x_2) \in \mathbb{R}^2$

$$\|qx_1\|\,\|qx_2\| \;\leq\; \psi(q) \text{ for infinitely many } q \in \mathbb{N}. \tag{7}$$

For example this shows that for almost every $(x_1, x_2) \in \mathbb{R}^2$ we can improve (1) to

$$\inf_{q\in\mathbb{N}} q(\log q)^2(\log\log q)\,\|qx_1\|\,\|qx_2\| \;=\; 0.$$

Although Gallagher's method does not readily apply to the mixed problems that we are considering, it has recently been shown using other techniques [2] that if p is a prime, if ψ is as above, and if (6) holds then for almost every $x \in \mathbb{R}$,

$$|q|_p\,\|qx\| \;\leq\; \psi(q) \text{ for infinitely many } q \in \mathbb{N}.$$

Here we will show how this result can be extended to non $p-$adic pseudo-absolute values $|\cdot|_{\mathcal{D}}$. The quality of approximation that we obtain will necessarily depend on the rate at which the sequence $\mathcal{D}$ grows. For this reason, given a pseudo-absolute value sequence $\mathcal{D}$ we define $\mathcal{M} : \mathbb{N} \to \mathbb{N} \cup \{0\}$ by $\mathcal{M}(N) = \max\{k : n_k \leq N\}$.

Theorem 2 ([7]). *Suppose that $\psi : \mathbb{N} \to \mathbb{R}$ is non-negative and decreasing and that $\mathcal{D} = \{n_k\}$ is a pseudo-absolute value sequence satisfying*

$$\sum_{k=1}^{\mathcal{M}(N)} \frac{\varphi(n_k)}{n_k} \gg \mathcal{M}(N) \text{ for all } N \in \mathbb{N}, \tag{8}$$

where φ denotes the Euler phi function. Then for almost all $x \in \mathbb{R}$ the inequality

$$|q|_{\mathcal{D}}\,\|qx\| \leq \psi(q) \tag{9}$$

has infinitely (resp. finitely) many solutions $q \in \mathbb{N}$ if the sum

$$\sum_{r=1}^{\infty} \mathcal{M}(r)\psi(r) \tag{10}$$

diverges (resp. converges).

We also note that when (10) converges the inequality (9) always has finitely many solutions. When $|\cdot|_D = |\cdot|_p$ for some prime p we have that $\mathcal{M}(N) \asymp \log N$, and Theorem 2 reduces in this case to the result from [2]. To see what Theorem 2 means in terms of the infima type expressions that occur in the Mixed Littlewood Conjecture, if $\mathcal{D}$ satisfies (8) then for almost every $x \in \mathbb{R}$ we have that

$$\inf_{q\to\infty} q\mathcal{M}(q)(\log q)(\log\log q)\,|q|_{\mathcal{D}}\,\|qx\| \;=\; 0,$$

while on the other hand for any $\epsilon > 0$ and for almost every $x \in \mathbb{R}$,

$$\inf_{q\to\infty} q\mathcal{M}(q)(\log q)(\log\log q)^{1+\epsilon}\,|q|_{\mathcal{D}}\,\|qx\| \;>\; 0.$$

Furthermore the hypothesis on $\mathcal{D}$ in Theorem 2 is not that restrictive in practice. Although it is possible to choose $\mathcal{D}$ so that (8) does not hold, any reasonably chosen pseudo-absolute value sequence should satisfy the condition. Examples include sequences $\mathcal{D}$ with bounded ratios or those whose elements of $\mathcal{D}$ are divisible only by some finite collection of primes.

References

[1] J. Bourgain, E. Lindenstrauss, P. Michel & A. Venkatesh, *Some effective results for $\times a \times b$*, Ergodic Theory Dynam. Systems **29** (2009), no. 6, 1705–1722.

[2] Y. Bugeaud, A. Haynes & S. Velani, *Metric considerations concerning the mixed Littlewood conjecture*, Int. J. Number Theory 7 (2011), no. 3, 593–609.

[3] M. Einsiedler, A. Katok & E. Lindenstrauss, *Invariant measures and the set of exceptions to Littlewood's conjecture*, Annals of Math. **164** (2006), 513–560.

[4] M. Einsiedler & D. Kleinbock, *Measure rigidity and p-adic Littlewood-type problems*, Compositio Math. **143** (2007), 689–702.

[5] H. Furstenberg, *Disjointness in ergodic theory, minimal sets, and a problem in Diophantine approximation*, Math. Systems Theory **1** (1967), 1–49.

[6] P.X. Gallagher, *Metric simultaneous Diophantine aproximations*, J. London Math. Soc. **37** (1962), 387–390.

[7] S. Harrap & A. Haynes, *The mixed Littlewood conjecture for pseudo absolute values*, (submitted). Preprint available at arxiv:1012.0191 (2011).

[8] B. de Mathan & O. Teuliè: *Problèmes Diophantiens simultanès*, Monatsh. Math. **143** (2004), 229–245.

Arithmetic applications of Hankel determinants

Wadim Zudilin
(joint work with Christian Krattenthaler, Tapani Matala-aho, Ville Merilä, Igor Rochev and Keijo Väänänen)

The second constant, after $\sqrt{2}$, we usually learn to be irrational is

$$e = \sum_{n=0}^{\infty} \frac{1}{n!},$$

Euler's constant. And the trick there is using the "obvious" rational approximations $p_n/q_n = \sum_{k=0}^{n-1} 1/k!$ and the fact

$$0 < q_n \left(e - \frac{p_n}{q_n} \right) < \frac{2}{n} \to 0 \quad \text{as } n \to \infty.$$

Later we realise we can do better with the Padé approximations for e^z, producing a sharp irrationality measure not only for e but also for e^r, $r \in \mathbb{Q} \setminus \{0\}$.

It comes as no surprise that the truncations and Padé approximations work well for a similar series

$$E_q(z) := \sum_{n=0}^{\infty} \frac{z^n}{(q-1)(q^2-1)\cdots(q^n-1)},$$

where for simplicity we assume $q \in \mathbb{Z}$, $q > 2$. Probably more surprising is that the "obvious" tail approximations lead one to an even stronger conclusion about the arithmetic of the values of $E_q(z)$ — their nonquadraticity — thanks to an original method of J.-P. Bézivin [2]. This is a consequence of our recent joint result [3] with C. Krattenthaler, I. Rochev and K. Väänänen; below I indicate some details of the construction taking $z = 1$ to avoid technicalities.

Introduce the normalised sequence of tails to $E_q(1)$,

$$v_n(x) := (q-1)(q^2-1)\cdots(q^n-1) \cdot \left(x - \sum_{k=0}^{n-1} \frac{1}{(q-1)(q^2-1)\cdots(q^k-1)} \right)$$

for $n = 0, 1, 2, \ldots$, and the related Hankel determinant

$$V_n(x) := \det_{0 \le i,j \le n} \big(v_{i+j}(x) \big) \in \mathbb{Z}[x],$$

which is a polynomial of degree at most $n+1$ in x. Then one expects $V_n(E_q(1))$ to be small, and indeed it can be shown that

$$\frac{\log |V_n(E_q(1))|}{\log q} \le -\frac{1}{3} n^3 + o(n^3) \quad \text{as } n \to \infty.$$

Note that $V_n(x)$ has a huge common factor of its coefficients of the form $q^{n(n^2-1)/6} \times \prod_{l<n/2} (q^l - 1)^{2(n-2l)}$, where the sharp form of the cyclotomic part in this expression is due to I. Rochev alone [9]. In other words,

$$\widehat{V}_n(x) := \frac{V_n(x)}{q^{n(n^2-1)/6} \prod_{l<n/2} (q^l-1)^{2(n-2l)}} \in \mathbb{Z}[x],$$

and an explicit information about the height of the polynomials together with their nonvanishing, at $x = E_q(1)$, for infinitely many indices n imply

Theorem 1 ([3]). *$E_q(1)$ is neither rational nor a quadratic irrationality.*

What is special here about dealing with (Hankel) determinants? First of all, the determinants are highly structured: the extra powers of q and the cyclotomic part are extracted using *different* elementary transformations of both rows *and* columns. Secondly, the nonvanishing (infinitely often) of the sequence $V_n(\lambda)$ for $\lambda \in \mathbb{R}$ is a consequence of Kronecker's rationality criterion: the property is equivalent to the rationality of the power series $\sum_{n=0}^{\infty} v_n(\lambda) z^n$.

The above construction works, although differently, for e and e^z (and even more general entire functions) but the arithmetic results in those cases are already known.

In our joint project [6] with T. Matala-aho and V. Merilä we extend Bézivin's method to the arithmetic study of the p-adic constants $\gamma = \gamma_p := \sum_{n=0}^{\infty} n!$ and related functions. The expected irrationality of γ is tied up with Wilf's conjecture [7] and Kurepa's conjecture [4] (a nonfixable gap in the proof given in [1] was recently observed by Yu. Nesterenko [8]).

In the newer settings, we let

$$v_n(x) := \frac{1}{n!} \cdot \left(x - \sum_{k=0}^{n-1} k! \right) \quad \text{for } n = 0, 1, 2, \ldots,$$

and normalise the related Hankel determinant $V_n(x) := \det_{0 \le i,j \le n} \big(v_{i+j}(x) \big)$ as follows: $\widehat{V}_n(x) := V_n(x)/\Lambda_n = x^{n+1} + \cdots \in \mathbb{Z}[x]$, where

$$\Lambda_n := \det_{0 \le i,j \le n} \left(\frac{1}{(i+j)!} \right) = (-1)^{n(n+1)/2} \frac{(n-1)\$\, n\$}{(2n)\$}$$

by means of the superfactorial notation $n\$:= \prod_{k=1}^{n} k!$. Then the height of the polynomial $\widehat{V}_n(x)$ is bounded above by $n\$\,(n+1)\$$. Because all

$$v_n(\gamma) = \sum_{k=0}^{\infty} (n+1)(n+2) \cdots (n+k)$$

are p-integral, we have $\operatorname{ord}_p V_n(\gamma) \ge 0$; a careful examination of the Hankel determinant produces a stronger conclusion: $\operatorname{ord}_p V_n(\gamma) \ge 2 \operatorname{ord}_p n\$$. Gathering all this information and the nonvanishing of $V_n(\gamma)$ infinitely often, we are able to show the following partial arithmetic result.

Theorem 2 ([6]). *Let $\mathcal{P}$ be a subset of primes such that*

$$\limsup_{n \to \infty} n\$^2 \prod_{p \in \mathcal{P}} |(2n)\$|_p < 1.$$

Given a rational number r, γ is not equal to r for at least one $p \in \mathcal{P}$.

Here $|\lambda|_p := p^{-\operatorname{ord}_p \lambda}$ denotes the p-adic absolute value of $\lambda \in \mathbb{Q}$. Note that the hypothesis of the theorem is roughly implied by $\limsup_{n \to \infty} n! \prod_{p \in \mathcal{P}} |(2n)!|_p = 0$

which can be then compared with the condition $\limsup_{n\to\infty} 4^n n! \prod_{p\in\mathcal{P}} |n!^2|_p < 1$; the latter may be obtained on using the Padé approximation technique [5].

We also observe (without proof) in [6] that the complex conjugate numbers

$$0.6971748832\ldots \pm i\, 1.1557273498\ldots$$

are accumulation points of some zeroes of the polynomials $V_n(x)$ as $n \to \infty$, which make them plausible archimedean reincarnations of γ, although the literature lacks of values for the divergent series $\sum_{n=0}^{\infty} n!$. In contrast, the series $\sum_{n=0}^{\infty}(-1)^n n! = 0.596347362\ldots$ was already summed by Euler, while the explicit expression is due to Hardy:

$$\sum_{n=0}^{\infty}(-1)^n n! = \int_0^{\infty} \frac{e^{-t}\,\mathrm{d}t}{1+t} = e\biggl(-\gamma - \sum_{n=1}^{\infty} \frac{(-1)^n}{n\cdot n!}\biggr).$$

References

[1] D. Barsky and B. Benzaghou, *Nombres de Bell et somme de factorielles*, J. Théor. Nombres Bordeaux **16** (2004), 1–17.

[2] J.-P. Bézivin, *Sur les propriétés arithmétiques d'une fonction entière*, Math. Nachr. **190** (1998), 31–42.

[3] C. Krattenthaler, I. Rochev, K. Väänänen and W. Zudilin, *On the non-quadraticity of values of the q-exponential function and related q-series*, Acta Arith. **136** (2009), 243–269.

[4] D. Kurepa, *On the left factorial function !n*, Math. Balkanica **1** (1971), 147–153.

[5] T. Matala-aho, *Type II Hermite–Padé approximations of generalized hypergeometric series*, Constr. Approx. **33** (2011), 289–312.

[6] T. Matala-aho, V. Merilä and W. Zudilin, *Arithmetic properties of the sum of factorials*, in progress.

[7] M. R. Murty and S. Sumner, *On the p-adic series $\sum_{n=1}^{\infty} n^k \cdot n!$*, Number theory, H. Kisilevsky and E. Z. Goren (eds.), CRM Proc. Lecture Notes **36** (Amer. Math. Soc., Providence, RI, 2004), 219–227.

[8] Yu. V. Nesterenko, *Private communication* (February 2011).

[9] I. P. Rochev, *On linear independence of values of certain q-series*, Izv. RAN. Ser. Mat. **75**:1 (2011), 181–224.

Arithmetic properties of p-adic elliptic polylogarithms and irrationality

Noriko Hirata-Kohno

1. Introduction

In this report, we introduce a p-adic elliptic polylogarithmic function to give a lower bound for the dimension of the linear space over the rationals spanned by 1 and values of the function. Our proof uses Padé approximation following the argument of T. Rivoal [10] and a new criterion due to Yu. V. Nesterenko [7]. We also show an example of the linear space of dimension ≥ 3 over $\mathbb{Q}$ generated by 1 and usual polylogarithms, by adapting a new linear independence criterion obtained by S. Fischler and W. Zudilin [2].

Let us recall the polylogarithmic function $\mathrm{L}i_s(z)$ $(s = 1, 2, \dots ,)$ defined by

$$\mathrm{L}i_s(z) = \sum_{k=1}^{\infty} \frac{z^k}{k^s}, z \in \mathbb{C}, |z| \leq 1 \ (z \neq 1 \text{ if } s = 1).$$

The function satisfies $\mathrm{L}i_1(z) = -\log(1-z)$ and $\mathrm{L}i_{s+1}(z) = \int_0^z \frac{\mathrm{L}i_s(t)}{t} dt$. Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, K be a number field of finite degree over $\mathbb{Q}$. Denote the ring of integers in K by $\mathfrak{O} = \mathfrak{O}_K$. We take a prime $p \in \mathbb{Q}$. For an Archimedean $v|\infty$, denote $|\cdot|_\infty = |\cdot|_v$, and for a finite place v of K over p, denote by $|\cdot|_v$ the normalized valuation such that $|x|_v = p^{-\mathrm{ord}_p(x)}$ for $x \in \mathbb{Q}$. Put $\mathbb{Q}_p$ the completion of $\mathbb{Q}$ by $v|p$ and K_v be the completion of K by v ($v|p$ or $v|\infty$). Write $n_v = [K_v : \mathbb{Q}_v]$ the local degree for v ($v|p$ or $v|\infty$). Finally set $\mathbb{C}_p$ the completion of the algebraic closure of K_v by $v|p$. We denote again by $|\cdot|_v$, the extension of $|\cdot|_v$ on $\mathbb{C}_p$ for $v|p$.

Let $\mathcal{E}$ be an elliptic curve defined by $y^2 = 4x^3 - g_2x - g_3$ $(g_2, g_3 \in K)$. Putting $X = x, Y = y/2$, $V = g_2/4, W = g_3/4$, $\mathcal{E}$ is defined by $Y^2 = X^3 - VX - W$. We may suppose $V, W \in \mathfrak{O}$; if either V or $W \notin \mathfrak{O}$, then there exists an integer $c \in \mathfrak{O}$ such that the elliptic curve $\mathcal{E}' : Y^2 = X^3 - V'X - W'$ with $V' = c^4V \in \mathfrak{O}$, $W' = c^6W \in \mathfrak{O}$ is isomorphic to $\mathcal{E}$, since the j-invariant remains equal. Denote by $h = h(\mathcal{E}) := \max\{1, h(1, V, W)\}$ the height of $\mathcal{E}$.

Let $\wp$ (resp. σ) be the Weierstraß elliptic function (resp. sigma function), associated with the period lattice $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ of $\mathcal{E}$. An elliptic logarithm of a point $P \in \mathcal{E} \hookrightarrow \mathbb{P}_2$ is a complex number u such that $P = (\sigma^3(u) : \wp(u)\sigma^3(u) : \wp'(u)\sigma^3(u))$.

Definition 1. *For a point $P = (X, Y, 1) \in \mathcal{E}$, introduce the local parameter at the origin: $t = t(P) = -X/Y, \omega(t) = -1/Y$. Define $\Omega(t) = dx/y = \wp'(z)dz/\wp'(z) = dz$ and $z = z(t) = \int \Omega(t)$. Then, $z(t)$ is viewed as a local reversed function of $t = -2\wp(z)/\wp'(z)$. We call $\log_{\mathcal{E}}(t) = z(t)$ an elliptic logarithmic function.*

Now we consider elliptic polylogarithmic function by doing a formal integral as follows.

Definition 2. *Let $t \in \mathbb{C}$ with $|t|_\infty < 1$. Define an s-th elliptic polylogarithmic function by $\mathrm{L}i_{\mathcal{E},1}(t) = \log_{\mathcal{E}}(t)$ and by*

$$\mathrm{L}i_{\mathcal{E},s}(t) = \int_0^t \frac{\mathrm{L}i_{\mathcal{E},s-1}(t)}{t} dt \ (s = 2, 3, \dots).$$

The Taylor expansion concerning with these functions is estimated as follows:

Lemma 1. *At the origin, the Taylor expansion of $\mathrm{L}i_{\mathcal{E},s}(t)$ $(s = 1, 2, 3, \dots)$ is given by*

$$\mathrm{L}i_{\mathcal{E},s}(t) = \sum_{k \geq 1} \frac{B_k}{k^s} t^k$$

where $B_1 = 1, B_k = \dfrac{C_k}{2}$, $C_k = \displaystyle\sum_{4\lambda+6\mu=k-1,\lambda,\mu\geq 0} b_{\lambda,\mu}^{(k)} V^\lambda W^\mu \quad (k \geq 1)$, $b_{\lambda,\mu}^{(k)} \in \mathbb{Z}$

and

$$|b_{\lambda,\mu}^{(k)}|_\infty \leq \frac{(2^5 \cdot 3 \cdot 5^2)^k}{(k+2)^3(\lambda+1)^3(\mu+1)^3} \quad (k \geq 1).$$

The height is bounded by $h(C_k) \leq 8.8k + (k-1)h$.

Let us now recall the Lutz-Weil p-adic elliptic function which corresponds to the p-adic version of the Weierstraß elliptic function $\wp$.

Put $\lambda_p = 1/(p-1)$ if $p \neq 2$, and $\lambda_2 = 3$. We set $\mathcal{C}_p := \{z \in \mathbb{C}_p \,:\, |z|_v < p^{-\lambda_p}\}$. There exist two solutions φ and $-\varphi$ to the differential equation $(\varphi')^2 = 1 - V\varphi^4 - W\varphi^6$ with $\varphi(0) = 0$, defined and analytic in $\mathcal{C}_p$. The function $\varphi(z)$ is called the Lutz-Weil p-adic elliptic function.

We then introduce a reversed function.

Definition 3. *By writing X, Y in terms of t and $\omega(t)$, consider the differential form $\Omega(t) = dX/2Y$, viewed as a formal power series in t. Define a p-adic elliptic logarithmic function by $\log_{p,\mathcal{E}}(t) = z(t) = \int \Omega(t)$.*

It is indeed a reversed function of $\exp_p(z) = \big(1/\varphi^2(z), -\varphi'(z)/\varphi^3(z), 1\big) = (t, -1, \omega(t))$.

The p-adic elliptic polylogarithmic function is also defined by a formal integral as follows.

Definition 4. *Let $t \in \mathbb{C}_p$ with $|t|_v < 1$. Define an s-th p-adic elliptic polylogarithmic function by $\mathrm{L}i_{p,\mathcal{E},1}(t) = \log_{p,\mathcal{E}}(t)$ and by*

$$\mathrm{L}i_{p,\mathcal{E},s}(t) = \int_0^t \frac{\mathrm{L}i_{p,\mathcal{E},s-1}(t)}{t} dt \ (s = 2, 3, \ldots).$$

We obtain exactly the same estimates as in the Archimedean case for the Taylor coefficients.

2. Linear independence of p-adic elliptic polylogarithms

We recall latest results concerning with irrationality of the values of (exponential) polylogarithmic function.

E. M. Nikišin [8] and M. Hata [3] investigated sufficient conditions such that for a rational number α, the values of polylogarithmic functions $\mathrm{L}i_1(\alpha), \mathrm{L}i_2(\alpha), \ldots, \mathrm{L}i_s(\alpha)$ and 1 are linearly independent over $\mathbb{Q}$.

In 2003, T. Rivoal [10] proved the following result.

Theorem A (Rivoal)**.** *Let s be an integer ≥ 2. Let $\alpha = a/b \in \mathbb{Q}$ with $a, b \in \mathbb{Z}$, $\gcd(a,b) = 1$ and $0 < |\alpha| < 1$. For any $\varepsilon > 0$, there exists an integer $A(\varepsilon, a, b) \geq 1$ satisfying the following property. If $s \geq A(\varepsilon, a, b)$, we have*

$$\dim_{\mathbb{Q}} \{\mathbb{Q} + \mathbb{Q}\mathrm{L}i_1(\alpha) + \cdots + \mathbb{Q}\mathrm{L}i_s(\alpha)\} \geq \frac{1-\varepsilon}{1+\log(2)} \log(s).$$

Rivoal proved Theorem A by using Nesterenko's linear independence criterion [6]. R. Marcovecchio [5] generalized Rivoal's result in the case of algebraic number field.

Now we suppose all the following conditions.

Assumptions: Let $K = \mathbb{Q}$ and $v = p$. Let $\beta = a/b, a, b \in \mathbb{Z}$, $\gcd(a, b) = 1$. Suppose $|\beta|_v < 1$ and $|V|_v = 1, |W|_v = 1$. Moreover, in the expression

$$\mathrm{L}i_{p,\mathcal{E},s}(t) = \sum_{k\geq 1} \frac{B_k}{k^s} t^k,$$

assume that we have $|B_k|_\infty = \mathcal{O}(k)$ for all $B_k (k \geq 1)$.

Theorem B (Nesterenko)**.** *Let c_1, c_2, τ_1, τ_2 be positive numbers with $\tau_2 \leq \tau_1$. Let $0 \leq \sigma(t)$ be a monotonically increasing function defined for all $t \geq t_0$ such that*

$$\lim_{t\to\infty} \sigma(t) = \infty,\ \limsup_{t\to\infty} \frac{\sigma(t+1)}{\sigma(t)} = 1.$$

Let $\xi = (\xi_1, \ldots \xi_m) \in \mathbb{C}_p^m - (0)$, and let $L_N(x_1, \ldots, x_m)$ be a sequence of linear forms with coefficients $\in \mathfrak{O}$ satisfying for all large N, denoting $|L_N|_\infty = \max$ of $|coefficients|_\infty$ of L_N;

$$\log |L_N|_\infty < \sigma(N), c_1 e^{-\tau_1 \sigma(N)} \leq \frac{|L_N(\xi)|_v}{|L_N|_v} \leq c_2 e^{-\tau_2 \sigma(N)}.$$

Then $\dim_{\mathbb{Q}} \{\mathbb{Q}\xi_1 + \cdots + \mathbb{Q}\xi_m\} \geq \dfrac{\tau_1}{[K : \mathbb{Q}] + \tau_1 - \tau_2}$.

By adapting Theorem B to the p-adic elliptic polylogarithmic function, we have:

Theorem 1. *Suppose all the assumptions above. Then for sufficiently large s, we have*

$$\dim_{\mathbb{Q}} \{\mathbb{Q} + \mathbb{Q}\mathrm{L}i_{p,\mathcal{E},1}(\beta) + \cdots + \mathbb{Q}\mathrm{L}i_{p,\mathcal{E},s}(\beta)\} \geq \mathcal{O}_{\mathcal{E},p,\beta}(1) \cdot \log s.$$

The constant $\mathcal{O}_{\mathcal{E},p,\beta}(1)$ can be explicitly calculated. However, our assumption for the growth of the coefficients of the Taylor expansion of the p-adic elliptic polylogarithmic function is indeed very strong.

3. Archimedean polylogarithms

We also present here a slight refinement of linear independence result concerning with the usual (exponential) polylogarithmic function, relying on a new linear independence criterion due to S. Fischler and W. Zudilin [2].

Theorem 2 (with H. Okada)**.** *Let $s \geq 356$. Then for $\alpha = a/b \in \mathbb{Q}$, with $a, b \in \mathbb{Z}$,* $\gcd(a, b) = 1,\ 0 < |\alpha| < 1,\ 1 \leq |a| \leq 49,\ 2 \leq |b| \leq 50$, *we have*

$$\dim_{\mathbb{Q}} \{\mathbb{Q} + \mathbb{Q}\mathrm{L}i_1(\alpha) + \cdots + \mathbb{Q}\mathrm{L}i_s(\alpha)\} \geq 3.$$

A more general statement is as follows.

Theorem 3 (with H. Okada). *Let s be an integer ≥ 2. Let $\alpha = a/b \in \mathbb{Q}$ with $a, b \in \mathbb{Z}$, $\gcd(a,b) = 1$ and $0 < |\alpha| < 1$. Put*

$$M = \dim_{\mathbb{Q}} \{\mathbb{Q} + \mathbb{Q}\mathrm{L}i_1(\alpha) + \cdots + \mathbb{Q}\mathrm{L}i_s(\alpha)\} - 1.$$

Let $r \in \mathbb{Z}$, $1 \leq r < M$ defined by

$$r = \max\left\{1, \left[\frac{M}{(\log\max\{3, M\})^{\rho}}\right]\right\}$$

where $\rho > 0$ arbitrarily chosen and fixed, with $[x]$ the largest integer part $\leq x$ (floor function). Then we have

$$M \geq \frac{\log r + \dfrac{(M-1)}{2} - \dfrac{\log|a|}{M} - \dfrac{r}{M}\log r}{1 + \log 2 + \dfrac{\log|b|}{M} + (\dfrac{r+1}{M})\log 2 + \dfrac{r}{M}\log r}\,.$$

We should note that the right-hand side of the conclusion of Theorem 3 contains M as in the statement in [2]. Indeed, when we subtract $\frac{M-1}{2}$ from the numerator of the right-hand side and add this part on the left-hand side, then it gives only an asymptotic formula for M.

References

[1] S. David and N. Hirata-Kohno, *Logarithmic Functions and Formal Groups of Elliptic Curves*, In: Diophantine Equations, (ed. N. Saradha), Tata Institute of Fundamental Research, Studies in Mathematics, Narosa Publishing House, 243–256, (2008).

[2] S. Fischler, W. Zudilin, *A refinement of Nesterenko's linear independence criterion with applications to zeta values*, Math. Ann., vol. 347, no. 4, 739–763, (2010).

[3] M. Hata, *On the linear independence of the values of polylogarithmic functions*, J. Math. Pures et Appl., vol. 69, 133–173, (1990).

[4] N. Hirata-Kohno, *Arithmetic properties of p-adic elliptic logarithmic functions*, Series on Number Theory and its Applications, vol. 7, (eds. Y. Hamahata, T. Ichikawa, A. Murase and T. Sugano), World Scientific, September, 110–119 (2011).

[5] R. Marcovecchio, *Linear independence of forms in polylogarithms*, Ann. Scuola Nor. Sup. Pisa CL. Sci., vol. 5, 1–11, (2006).

[6] Yu. V. Nesterenko, *On the linear independence of numbers*, Vestnik Moskov. Univ. Ser. I, Mat. Mekh. vol. 1, 46–49, (1985), English translation: Moscow Univ. Math. Bull. vol. 40, no. 1, 69–74, (1985).

[7] Yu. V. Nesterenko, *On a criterion of linear independence of p-adic numbers*, Manuscripta Math., to appear.

[8] E. M. Nikišin, *On irrationality of the values of the functions $F(x,s)$*, Mat. Sbornik vol. 109(151), no. 3(7), 410–417, (1979), English translation: Math. USSR Sbornik vol. 37, no.3, 381–388, (1980).

[9] J. Oesterlé, *Polylogarithmes*, Séminaire N. Bourbaki, no. 762, 49–67, (1992-1993).

[10] T. Rivoal, *Indépendance linéaire des valeurs des polylogarithmes*, J. Théorie des Nombres de Bordeaux vol. 15, no.2, 551–559, (2003).

Infinite Non-Abelian Extensions and Small Heights

Philipp Habegger

Let $h(\alpha)$ denote the absolute, logarithmic Weil height of $\alpha \in \overline{\mathbf{Q}}$, where $\overline{\mathbf{Q}}$ denotes an algebraic closure of $\mathbf{Q}$. If $P = a_d T^d + \cdots + a_0 \in \mathbf{Z}[X]$ is the unique polynomial of minimal degree such that $P(\alpha) = 0$, the $a_0, \ldots, a_d$ coprime, and $a_d > 0$, then

$$h(\alpha) = \frac{1}{d} \log \left(a_d \prod_{P(z)=0} \max\{1, |z|\} \right)$$

where the product runs over all complex roots of P.

For example $h(2^{1/n}) = (\log 2)/n$ tends to zero as n runs over all positive integers.

A theorem often attributed to Northcott implies that any set of algebraic numbers with bounded height and bounded degree is finite. Hence for any number field K there exists $\epsilon = \epsilon_K > 0$ such that if $\alpha \in K$ then either

$$h(\alpha) = 0 \quad \text{or} \quad h(\alpha) \geq \epsilon.$$

Schinzel [7] proved that $\mathbf{Q}^{\mathrm{mr}}$, the composite in $\overline{\mathbf{Q}}$ of all totally real number fields, admits a similar height gap. More precisely, if $\alpha \in \mathbf{Q}^{\mathrm{mr}}$ with $\alpha \neq 0, \pm 1$, then

$$h(\alpha) \geq \frac{1}{2} \log \left(\frac{\sqrt{5}+1}{2} \right)$$

and this inequality is sharp.

We will say that a subfield F of $\overline{\mathbf{Q}}$ satisfies the Bogomolov property if there exists $\epsilon > 0$ such that

$$\text{if} \quad \alpha \in F \quad \text{then} \quad h(\alpha) = 0 \quad \text{or} \quad h(\alpha) \geq \epsilon.$$

This property was named by Bombieri and Zannier [4]. They showed that if p is a prime, then any Galois extension of $\mathbf{Q}$ that admits an embedding into a finite extension of the p-adics satisfies the Bogomolov property. Their result can thus be view as a p-adic version of Schinzel's Theorem.

Instead of imposing a local restriction, Amoroso and Dvornicich [1] proved that the maximal abelian extension $\mathbf{Q}^{\mathrm{ab}}$ of $\mathbf{Q}$ satisfies the Bogomolov property. They obtained $(\log 5)/12$ as a lower bound for the gap. In later work, Amoroso and Zannier [2] showed that the maximal abelian extension of an arbitrary number field satisfies the Bogomolov property.

The classical Theorem of Kronecker-Weber states that $\mathbf{Q}^{\mathrm{ab}}$ is generated as a field by all roots of unity. This can be reformulated as stating that $\mathbf{Q}^{\mathrm{ab}}$ is the field generated by the points of finite order of the algebraic group $\mathbf{G}_m$.

Starting from this interpretation of $\mathbf{Q}^{\mathrm{ab}}$ it seems natural to consider fields generated by all points of finite order of other commutative algebraic groups. To this extent let E be an elliptic curve given by a Weierstrass equation $y^2 = x^3 + ax + b$ with rational coefficients a and b. We let E_{tors} denote the group of all points in $E(\overline{\mathbf{Q}})$ of finite order. The problem is thus to determine if the field $\mathbf{Q}(E_{\mathrm{tors}})$ generated by the x- and y-coordinates of all non-zero elements in E_{tors} has the

Bogomolov property. We note that $\mathbf{Q}(E_{\text{tors}})$ is an infinite Galois extension of $\mathbf{Q}$. Indeed, properties of the Weil pairing imply that $\mathbf{Q}(E_{\text{tors}})$ contains $\mathbf{Q}^{\text{ab}}$.

If E has potential complex multiplications by an order in an imaginary quadratic number field K, then $\mathbf{Q}(E_{\text{tors}})$ is in the maximal abelian extension on K. In this case, the result of Amoroso and Zannier implies that $\mathbf{Q}(E_{\text{tors}})$ satisfies the Bogomolov property.

So suppose that E does not have potential complex multiplications. By Serre's Open Image Theorem [8] the group $\text{Gal}(\mathbf{Q}(E_{\text{tors}})/\mathbf{Q})$ is isomorphic to an open subgroup of $\text{GL}_2(\widehat{\mathbf{Z}})$, with $\widehat{\mathbf{Z}}$ the Prüfer ring. Amoroso and Zannier's result is not applicable to $\mathbf{Q}(E_{\text{tors}})$ as $\text{GL}_2(\widehat{\mathbf{Z}})$ does not contain an open abelian subgroup. Moreover, neither Schinzel's Theorem nor Bombieri and Zannier's p-adic analog may be applied. But $\mathbf{Q}(E_{\text{tors}}) \supset \mathbf{Q}^{\text{ab}}$ and so both fields have unbounded ramification above all primes.

In my talk I presented the following result [6].

Theorem 1. *The field $\mathbf{Q}(E_{\text{tors}})$ satisfies the Bogomolov property.*

I then gave a short overview of the proof which makes use of the following theorem of Elkies [5]. There exist infinitely many primes where E has supersingular reduction. This remarkable result is currently not known to hold for elliptic curves defined over an arbitrary number field.

In order to show that $\mathbf{Q}(E_{\text{tors}})$ satisfies the Bogomolov property we must fix one supersingular prime p which is sufficiently large with respect to E. For example, we require the natural modulo p Galois representation attached to E to be surjective. Serre's Theorem guarantees this for all sufficiently large p. The proof of the height lower bound is then based on a local metric argument at places above p using, among other things, Lubin-Tate Theory. The argument makes essential use of supersingularity. Roughly speaking, the product formula can be used to combine the non-Archimedean estimates above p with estimates at Archimedean places coming from Bilu's Equidistribution Theorem [3]. After a descent argument this leads to a proof that $\mathbf{Q}(E_{\text{tors}})$ satisfies the Bogomolov property.

References

[1] F. Amoroso and R. Dvornicich, *A lower bound for the height in abelian extensions*, J. Number Theory **80** (2000), no. 2, 260–272.
[2] F. Amoroso and U. Zannier, *A relative Dobrowolski lower bound over abelian extensions*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **29** (2000), no. 3, 711–727.
[3] Y. Bilu, *Limit distribution of small points on algebraic tori*, Duke Math. J. **89** (1997), no. 3, 465–476.
[4] E. Bombieri and U. Zannier, *A note on heights in certain infinite extensions of* $\mathbb{Q}$, Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl. **12** (2001), 5–14 (2002).
[5] N.D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* **Q**, Invent. Math. **89** (1987), no. 3, 561–567.
[6] P. Habegger. Small Height and Infinite Non-Abelian Extensions. *Preprint* `arXiv:1109.5859v1`, 2011.
[7] A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number*, Acta Arith. **24** (1973), 385–399.

[8] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

Diophantine exponents and parametric geometry of numbers

Oleg N. German

Let Θ be an $n \times m$ real matrix. The supremum of the real numbers γ such that the inequality

$$|\Theta \mathbf{x} - \mathbf{y}| \leqslant |\mathbf{x}|^{-\gamma} \tag{1}$$

has infinitely many non-zero solutions in $\mathbf{z} = (\mathbf{x}, \mathbf{y}) \in \mathbb{Z}^m \oplus \mathbb{Z}^n$ is called the *(regular) Diophantine exponent* of Θ and is denoted by $\beta(\Theta)$.

Substituting (1) by the inequalities

$$|\mathbf{x}| \leqslant t, \qquad |\Theta \mathbf{x} - \mathbf{y}| \leqslant t^{-\gamma} \tag{2}$$

and requiring (2) to have a non-zero solution $\mathbf{z} = (\mathbf{x}, \mathbf{y}) \in \mathbb{Z}^m \oplus \mathbb{Z}^n$ for *all* sufficiently large t, gives us the uniform analogue of $\beta(\Theta)$, which is called the *uniform Diophantine exponent* of Θ and is denoted by $\alpha(\Theta)$.

These two quantities measure how well the space

$$\mathcal{L} = \left\{ \mathbf{z} = (\mathbf{x}, \mathbf{y}) \in \mathbb{R}^{m+n} \,\middle|\, \Theta \mathbf{x} = \mathbf{y} \right\}$$

of solutions to the system $\Theta \mathbf{x} = \mathbf{y}$ can be approximated with one-dimensional rational subspaces of $\mathbb{R}^{m+n}$.

Our aim is to discuss two ways of generalizing the quantities $\beta(\Theta)$, $\alpha(\Theta)$ to the case of approximating $\mathcal{L}$ by p-dimensional rational subspaces. One way is to require (2) to have p linearly independent solutions. This immediately gives us exponents $\beta_p(\Theta)$ and $\alpha_p(\Theta)$. Another way is to estimate the order of approximation in terms of the height of the approximating subspace. This approach gives us exponents $\mathfrak{b}_p(\Theta)$ and $\mathfrak{a}_p(\Theta)$. Namely, $\mathfrak{b}_p(\Theta)$ is the supremum of the real numbers γ such that the inequality

$$\max_{\substack{\mathbf{L} \in \wedge^{1+k}(\mathcal{L}) \\ |\mathbf{L}|=1}} |\mathbf{L} \wedge \mathbf{Z}| \leqslant |\mathbf{Z}|^{-\gamma} \tag{3}$$

has infinitely many nonzero solutions in $\mathbf{Z} \in \wedge^p(\mathbb{Z}^{m+n})$, where $k = \max(0, m-p)$. The exponent $\mathfrak{a}_p(\Theta)$ is obtained by substituting (3) with

$$|\mathbf{Z}| \leqslant t, \qquad \max_{\substack{\mathbf{L} \in \wedge^{1+k}(\mathcal{L}) \\ |\mathbf{L}|=1}} |\mathbf{L} \wedge \mathbf{Z}| \leqslant t^{-\gamma} \tag{4}$$

and requiring (4) to have a non-zero solution $\mathbf{Z} \in \wedge^p(\mathbb{Z}^{m+n})$ for *all* t large enough.

It was shown in [1] that $\mathfrak{b}_1(\Theta) = \beta_1(\Theta) = \beta(\Theta)$ and $\mathfrak{a}_1(\Theta) = \alpha_1(\Theta) = \alpha(\Theta)$, so the exponents $\beta_p(\Theta)$, $\alpha_p(\Theta)$, $\mathfrak{b}_p(\Theta)$, $\mathfrak{a}_p(\Theta)$ are indeed a generalization of $\beta(\Theta)$ and $\alpha(\Theta)$.

A very useful point of view at these phenomena is provided by so called *parametric geometry of numbers* devised lately by W. M. Schmidt and L. Summerer [2], [3]. It connects Θ to a certain one-parametric family of parallelepipeds $\mathcal{B}(s)$

and studies the asymptotic behaviour of their successive minima with respect to an appropriately chosen lattice. In order to describe it let us introduce certain notation.

Let $d = m + n$, let $\mathcal{B}_\infty^d$ be the unit ball in the sup-norm in $\mathbb{R}^d$, let

$$\mathcal{B}(s) = \begin{pmatrix} e^{\tau_1(s)} & 0 & \cdots & 0 \\ 0 & e^{\tau_2(s)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e^{\tau_d(s)} \end{pmatrix} \mathcal{B}_\infty^d,$$

where $\tau_1(s) = \ldots = \tau_m(s) = s,\ \tau_{m+1}(s) = \ldots = \tau_d(s) = -ms/n$, and let

$$\Lambda = \begin{pmatrix} E_m & 0 \\ \Theta & E_n \end{pmatrix}^{-1} \mathbb{Z}^d,$$

where E_n, E_m are corresponding unity matrices.

Schmidt–Summerer's exponents are defined as

$$\underline{\psi}_p(\Theta) = \liminf_{s\to+\infty} \frac{\ln(\lambda_p(\mathcal{B}(s)))}{s}, \qquad \overline{\psi}_p(\Theta) = \limsup_{s\to+\infty} \frac{\ln(\lambda_p(\mathcal{B}(s)))}{s}$$

and

$$\underline{\Psi}_p(\Theta) = \liminf_{s\to+\infty} \frac{\ln\left(\prod_{i=1}^{p} \lambda_i(\mathcal{B}(s))\right)}{s}, \qquad \overline{\psi}_p(\Theta) = \limsup_{s\to+\infty} \frac{\ln\left(\prod_{i=1}^{p} \lambda_i(\mathcal{B}(s))\right)}{s},$$

where $\lambda_i(\mathcal{B}(s))$ is the i-th successive minimum of $\mathcal{B}(s)$ with respect to Λ.

It was shown in [1] that Schmidt–Summerer's exponents are connected to the intermediate Diophantine exponents by the relations

$$(1 + \beta_p(\Theta))(1 + \underline{\psi}_p(\Theta)) = (1 + \alpha_p(\Theta))(1 + \overline{\psi}_p(\Theta)) = 1 + m/n,$$

$$(1 + \mathfrak{b}_p(\Theta))(\varkappa_p + \underline{\Psi}_p(\Theta)) = (1 + \mathfrak{a}_p(\Theta))(\varkappa_p + \overline{\psi}_p(\Theta)) = 1 + m/n,$$

where $\varkappa_p = \min(p, \frac{m}{n}(m + n - p))$.

Our ultimate goal is to describe the existing inequalities between the intermediate Diophantine exponents (and hence between Schmidt–Summerer's exponents) obtained by W. M. Schmidt in [4], by M. Laurent, Y. Bugeaud in [5], W. M. Schmidt, L. Summerer in [3] and by the author in [1]. One of the remarkable features of those inequalities is that they refine in many ways well known transference theorems, which connect the Diophantine exponents of Θ and $\Theta^\intercal$.

Among such inequalities are

$$(5) \qquad \begin{aligned} (d - p - 1)(1 + \mathfrak{b}_{p+1}(\Theta)) &\geqslant (d - p)(1 + \mathfrak{b}_p(\Theta)), \\ (d - p - 1)(1 + \mathfrak{a}_{p+1}(\Theta)) &\geqslant (d - p)(1 + \mathfrak{a}_p(\Theta)) \end{aligned}$$

holding for $p \geqslant m$, and

$$(6) \qquad \begin{aligned} (d - p - 1)(1 + \mathfrak{b}_p(\Theta))^{-1} &\geqslant (d - p)(1 + \mathfrak{b}_{p+1}(\Theta))^{-1} - n, \\ (d - p - 1)(1 + \mathfrak{a}_p(\Theta))^{-1} &\geqslant (d - p)(1 + \mathfrak{a}_{p+1}(\Theta))^{-1} - n \end{aligned}$$

holding for $p < m-1$, which refine Dyson's transference inequality

$$\mathfrak{b}_1(\Theta^{\intercal}) \geqslant \frac{n\mathfrak{b}_1(\Theta)+n-1}{(m-1)\mathfrak{b}_1(\Theta)+m}\,.$$

We also mention the inequalities

$$\mathfrak{b}_2(\Theta) \geqslant \frac{\mathfrak{b}_1(\Theta)+\mathfrak{a}_1(\Theta)}{1-\mathfrak{a}_1(\Theta)}, \qquad \mathfrak{a}_2(\Theta) \geqslant (1-\mathfrak{a}_1(\Theta))^{-1} - \frac{n-2}{n-1}$$

holding for $m = 1$ (for the former we must also suppose that $\mathcal{L} \cap \mathbb{Z}^d$ is not one-dimensional) and

$$\mathfrak{b}_2(\Theta) \geqslant \begin{cases} \dfrac{\mathfrak{a}_1(\Theta)-1}{2+\mathfrak{b}_1(\Theta)-\mathfrak{a}_1(\Theta)}\,, & \text{if } \ \mathfrak{a}_1(\Theta) \neq \infty, \\ \dfrac{1-\mathfrak{a}_1(\Theta)^{-1}}{\mathfrak{b}_1(\Theta)^{-1}+\mathfrak{a}_1(\Theta)^{-1}}\,, & \end{cases}$$

and

$$\mathfrak{a}_2(\Theta) \geqslant \begin{cases} \dfrac{n-1}{-n-(d-2)(1-\mathfrak{a}_1(\Theta))^{-1}}\,, & \text{if } \ \mathfrak{a}_1(\Theta) \leqslant 1, \\ \dfrac{m-1}{n+(d-2)(\mathfrak{a}_1(\Theta)-1)^{-1}}\,, & \text{if } \ \mathfrak{a}_1(\Theta) \geqslant 1 \end{cases}$$

holding for $m \geqslant 2$. These inequalities combined with (5) and (6) give

$$\mathfrak{b}_1(\Theta^{\intercal}) \geqslant \begin{cases} \dfrac{(n-1)(1+\mathfrak{b}_1(\Theta))-(1-\mathfrak{a}_1(\Theta))}{(m-1)(1+\mathfrak{b}_1(\Theta))+(1-\mathfrak{a}_1(\Theta))}\,, & \text{if } \ \mathfrak{a}_1(\Theta) \neq \infty, \\ \dfrac{(n-1)(1+\mathfrak{b}_1(\Theta)^{-1})-(\mathfrak{a}_1(\Theta)^{-1}-1)}{(m-1)(1+\mathfrak{b}_1(\Theta)^{-1})+(\mathfrak{a}_1(\Theta)^{-1}-1)} & \end{cases}$$

and

$$\mathfrak{a}_1(\Theta^{\intercal}) \geqslant \begin{cases} \dfrac{n-1}{m-\mathfrak{a}_1(\Theta)}, & \text{if } \ \mathfrak{a}_1(\Theta) \leqslant 1, \\ \dfrac{n-\mathfrak{a}_1(\Theta)^{-1}}{m-1}, & \text{if } \ \mathfrak{a}_1(\Theta) \geqslant 1. \end{cases}$$

Finally, we turn to Schmidt and Summerer's inequalities

$$\alpha_p \leqslant \frac{\beta_p}{1+\beta_1-\beta_p} \quad \text{and} \quad \beta_p \geqslant \frac{\alpha_p}{1+\alpha_d-\alpha_p}\,.$$

Acknowledgements. This research was supported by RFBR (grant N° 09–01–00371a) and by the grant of the President of Russian Federation N° MK–5016.2012.1.

References

[1] O. N. German *Intermediate Diophantine exponents and parametric geometry of numbers.* Acta Arithmetica, to appear (2012), preprint available at arXiv:1106.2353.

[2] W. M. Schmidt, L. Summerer *Parametric geometry of numbers and applications.* Acta Arithmetica, **140**:1, 67–91 (2009).

[3] W. M. Schmidt, L. Summerer *Diophantine approximation and parametric geometry of numbers.* Monatsh. Math., to appear (2012), DOI 10.1007/s00605-012-0391-z.
[4] W. M. Schmidt *On heights of algebraic subspaces and diophantine approximations.* Annals of Math. 85:3 (1967), 430–472.
[5] Y. Bugeaud, M. Laurent *On transfer inequalities in Diophantine approximation, II.* Math. Z., 265:2 (2010), 249–262.

The generalized superelliptic equation

Michael A. Bennett
(joint work with Sander Dahmen)

If $F(x, y) \in \mathbb{Z}[x, y]$ is an irreducible binary form of degree $k \geq 3$ then a theorem of Darmon and Granville implies that the generalized superelliptic equation

$$F(x, y) = z^l$$

has, given an integer $l \geq \max\{2, 7-k\}$, at most finitely many solutions in coprime integers x, y and z. In our talk, we describe how this result can be extended to the case where the parameter l is now taken to be variable, for large classes of cubic forms (and certain forms of higher degree). In the case of irreducible cubic forms, this provides the first examples where such a conclusion has been proven. The method of proof combines classical invariant theory, modular Galois representations, and properties of elliptic curves with isomorphic mod n Galois representations. In the course of constructing an infinite family of cubic forms with this property, we are led to explicitly solve an infinite family of Thue-Mahler equations.

References

[1] M. Bennett and S. Dahmen, *Klein forms and the generalized superelliptic equation*, Ann. Math., to appear.

Reporter: Clemens Fuchs

Participants

Prof. Dr. Boris Adamczewski
Dept. de Mathematiques
Universite Claude Bernard Lyon I
43, Bd. du 11 Novembre 1918
F-69622 Villeurbanne Cedex

Prof. Dr. Francesco Amoroso
Dept. de Mathematiques
Universite de Caen
F-14032 Caen Cedex

Dr. Dzmitry Badziahin
Dept. of Mathematical Sciences
Durham University
Science Laboratories
South Road
GB-Durham DH1 3LE

Prof. Dr. Michael A. Bennett
Department of Mathematics
University of British Columbia
121-1984 Mathematics Road
Vancouver BC V6T 1Z2
CANADA

Prof. Dr. Victor Beresnevich
Department of Mathematics
University of York
GB-Heslington, York Y010 5DD

Prof. Dr. Yann Bugeaud
Institut de Mathematiques
Universite de Strasbourg
7, rue Rene Descartes
F-67084 Strasbourg Cedex

Prof. Dr. Pietro Corvaja
Dip. di Matematica e Informatica
Universita di Udine
Via delle Scienze 208
I-33100 Udine

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

Prof. Dr. Oleg German
Mechanical and Mathematical Faculty
Moscow State University
Department of Mathematics (TFFA)
Leninskie Gory
Moscow 119 992
RUSSIA

Dr. Philipp Habegger
Institut für Mathematik
Goethe-Universität Frankfurt
Robert-Mayer-Str. 6-10
60325 Frankfurt am Main

Dr. Stephen Harrap
Matematisk Institut
Aarhus Universitet
Ny Munkegade 118
DK-8000 Aarhus C

Prof. Dr. Noriko Hirata-Kohno
College of Science and Technology
Nihon University
1-8, Suraga-dai, Kanda
Tokyo 101-8308
JAPAN

Dr. Tünde Kovacs
Institute of Mathematics
University of Debrecen
Pf. 12
H-4010 Debrecen

Prof. Dr. Michel Laurent
Institut de Mathematiques de Luminy
Case 907
163 Avenue de Luminy
F-13288 Marseille Cedex 9

Prof. Dr. Raffaele Marcovecchio
Fakultät für Mathematik
Universität Wien
Nordbergstr. 15
A-1090 Wien

Prof. Dr. Nikolay K. Moshchevitin
Department of Mechanics & Mathematics
Moscow State University
Leninskie Gory, 1
119 992 Moscow
RUSSIA

Prof. Dr. Yuri V. Nesterenko
Faculty of Mechanics and Mathematics
Moscow State University
Lenin Hills 1
119899 Moscow
RUSSIA

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
Dept. de Mathematiques
Universite Claude Bernard Lyon I
43, Bd. du 11 Novembre 1918
F-69622 Villeurbanne Cedex

Prof. Dr. Damien Roy
Department of Mathematics & Statistics
University of Ottawa
585 King Edward Avenue
Ottawa , Ont. K1N 6N5
CANADA

Prof. Dr. Cameron L. Stewart
Dept. of Pure Mathematics
University of Waterloo
200 University Avenue West
Waterloo , Ont. N2L 3G1
CANADA

Dr. Sanju Velani
Department of Mathematics
University of York
GB-Heslington, York Y010 5DD

Prof. Dr. Carlo Viola
Dip. di Matematica "L.Tonelli"
Universita di Pisa
Largo Bruno Pontecorvo, 5
I-56127 Pisa

Dr. Martin Widmer
Scuola Normale Superiore di Pisa
Piazza dei Cavalieri 7
I-56126 Pisa

Prof. Dr. Wadim Zudilin
School of Mathematical and
Physical Sciences
University of Newcastle
Callaghan NSW 2308
AUSTRALIA