Mathematisches Forschungsinstitut Oberwolfach

Report No. 21/2016

DOI: 10.4171/OWR/2016/21

Diophantische Approximationen

Organised by
Yann Bugeaud, Strasbourg
Philipp Habegger, Basel
Umberto Zannier, Pisa

10 April – 16 April 2016

Abstract. This number theoretic conference was focused on a broad variety of subjects in (or closely related to) Diophantine approximation, including the following: metric Diophantine approximation, Mahler's method in transcendence, geometry of numbers, theory of heights, arithmetic dynamics, function fields arithmetic.

Mathematics Subject Classification (2010): 11Jxx, 11K60.

Introduction by the Organisers

The workshop *Diophantische Approximationen* (Diophantine approximations), organised by Yann Bugeaud (Strasbourg), Philipp Habegger (Basel), and Umberto Zannier (Pisa) was held April 10th - April 16th, 2016. There have been 51 participants with broad geographic representation and a large variety of mathematical backgrounds. Young researchers were well represented, including among the speakers. Below we briefly recall the topics discussed, thus outlining some of the modern lines of investigation in Diophantine approximation and closely related areas. We refer the reader to the abstracts for more details.

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. Irrationality and transcendence have been discussed in the talks of Viola and Zudilin. Slightly related is the parametric geometry of numbers, recently introduced by W. Schmidt and Summerer, and which was at the heart of the talk of Roy.

Metric Diophantine approximation has seen great advances during the last decade and was present in the talks of Badziahin, Beresnevich, Haynes and Moshchevitin.

At the end of the 1920s, Kurt Mahler introduced the so-called *Mahler's method* to give new transcendence results. It has been recently revisited and several new advances were presented by Bell, Philippon and Zorin. A fourth related talk, on E- and G-functions was given by Rivoal.

Questions on algebraic number fields and on the theory of heights have been discussed by Widmer (with a connection to decidability questions), Amoroso, and Pottmeyer. Heights also played a role in Gaudron's talk. He presented explicit lower bounds for the Néron-Tate height on an abelian variety. Silverman discussed the vanishing locus of the Néron-Tate height attached to nef line bundles, a weakening of the ampleness criterion. Hindry presented evidence why the regulator and the Tate-Shafarevich group of an abelian variety are difficult to compute in the number and function field setting. Pazuki discussed the Northcott property for the regulator of an abelian variety. Kühne's talk was on a height bound for just likely intersections in semi-abelian varieties.

Bilu showed a strengthened estimate for the number of fields generated by fibers of rational functions over curves over integral values.

Bertrand spoke on Kummer theory for abelian varieties over a function field.

Functional transcendence in the spirit of the Ax-Schanuel Theorem played an important role in Corvaja's and Gao's talks. Corvaja discussed applications of Manin's Theorem of the Kernel and beyond to Pink's Conjecture on families of abelian varieties. Gao put the functional Schanuel Conjecture in a very general context and presented evidence in the case of a vectorial extension of an abelian variety. Harry Schmidt presented solvability results on the polynomial Pell equation.

Diophantine equations remain a subject of constant interest. Bennett combined a large variety of techniques to list integer squares with very few digits in some given base. Akhtari explained that many Thue equations have no solutions. Levin presented progress towards effective Shafarevich for genus 2 curves.

Various questions coming from ergodic theory and with a Diophantine flavour were discussed by Varju and Lindenstrauss.

Arithmetic dynamics is a quite recent topic of growing interest among the participants, and was the subject of the talks of Ingram, Tucker, and Zieve. Ingram exhibited a non-trivial family of non-Lattès maps that satisfy the Morton-Silverman uniformity conjecture. Tucker presented a dynamical analog of the Bugeaud-Corvaja-Zannier gcd bounds by taking composition of functions instead of powers of numbers. Zieve spoke on a variant of the Mordell-Lang Conjecture in the dynamical setting.

The abstracts are listed by order of appearance of the speakers during the conference.

Acknowledgement: The MFO and the workshop organizers would like to thank the National Science Foundation for supporting the participation of junior researchers in the workshop by the grant DMS-1049268, "US Junior Oberwolfach Fellows".

Workshop: Diophantische Approximationen

Table of Contents

Tanguy Rivoal (joint with Stéphane Fischler and Julien Roques)
Arithmetic theory of E-operators 1105

Patrice Philippon
Values of Mahler functions and Galois theory 1109

Jason Bell (joint with Yann Bugeaud and Michael Coons)
Diophantine approximation of Mahler numbers 1112

Evgeniy Zorin
Measures of algebraic independence and Diophantine properties of Mahler numbers and their generalizations. 1114

Joseph H. Silverman (joint with Shu Kawaguchi)
New Positivity Results for Canonical Heights on Abelian Varieties and an Application to Arithmetic Dynamics 1118

Éric Gaudron (joint with Vincent Bosser)
Lower bound for the Néron-Tate height 1120

Fabien Pazuki
Northcott property for the regulators of number fields and abelian varieties 1122

Péter P. Varjú (joint with E. Breuillard)
Some Diophantine questions motivated by random walks 1125

Elon Lindenstrauss
Around Furstenberg's $\times 2 \times 3$ theorem 1127

Victor Beresnevich (joint with R. C. Vaughan, S. Velani, E. Zorin)
Simultaneous rational approximations to manifolds 1128

Nikolay Moshchevitin
Diophantine Approximation with quadratic forms 1130

Daniel Bertrand
Kummer theory on abelian varieties over function fields 1132

Pietro Corvaja (joint with Y. André, D. Masser, U. Zannier)
Torsion subvarieties and Betti maps 1136

Ziyang Gao
Bi-algebraic system on the universal vectorial extension 1137

Lukas Pottmeyer (joint with Paul Fili)
Height bounds for algebraic numbers under splitting conditions 1141

Thomas J. Tucker
Compositional analogs of the Bugeaud-Corvaja-Zannier theorem, and applications 1143

Martin Widmer
Property (N), Decidability and Diophantine Approximation 1145

Harry Schmidt
Pell's equation in polynomials and additive extensions 1147

Damien Roy
Remarks on the topology of Diophantine approximation Spectra 1149

Michael Bennett (joint with Adrian Scheerer)
Squares with three nonzero digits 1152

Michael E. Zieve (joint with Trevor Hyde)
An arithmetic dynamical analogue of the Mordell–Lang conjecture 1153

Patrick Ingram
Heights and preperiodic points for certain polynomials 1156

Yuri Bilu (joint with Florian Luca)
Diversity in Parametric Families of Number Fields 1158

Lars Kühne
The Bounded Height Conjecture for semiabelian varieties 1160

Marc Hindry (joint with Amílcar Pacheco)
Brauer-Siegel estimates for abelian varieties 1163

Wadim Zudilin
Determinants and irrationality 1166

Carlo Viola (joint with F. Pinna)
The saddle-point method in $\mathbb{C}^N$ 1168

Alan Haynes (joint with Henna Koivusalo, James Walton)
An application of Diophantine approximation to regularity of patterns in cut and project sets 1171

Dzmitry Badziahin
How should potential counterexamples to p-adic Littlewood conjecture look like? 1173

Aaron Levin
Integral points and the Shafarevich conjecture for abelian surfaces 1176

Shabnam Akhtari (joint with Manjul Bhargava)
Many Thue equations have no solutions 1178

Francesco Amoroso (joint with David Masser)
Lower bounds for the height in Galois extension 1180

Abstracts

Arithmetic theory of *E*-operators

Tanguy Rivoal
(joint work with Stéphane Fischler and Julien Roques)

In my talk, I presented results obtained with Stéphane Fischler (Université Paris Sud) and, independently, with Julien Roques (Université Grenoble Alpes).

Definition 1. An E-function is a power series $E(z) = \sum_{n=0}^{\infty} \frac{a_n}{n!} z^n$ such that $a_n \in \overline{\mathbb{Q}}$ and there exists $C > 0$ such that:

(i) For any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and any $n \geq 0$, $|\sigma(a_n)| \leq C^{n+1}$.

(ii) There exists a sequence of rational integers $d_n \neq 0$, with $|d_n| \leq C^{n+1}$, such that $d_n a_m$ is an algebraic integer for all $m \leq n$.

(iii) $E(z)$ satisfies a homogeneous linear differential equation with coefficients in $\overline{\mathbb{Q}}(z)$.

A power series $\sum_{n=0}^{\infty} a_n z^n$ is a G-function if and only if $\sum_{n=0}^{\infty} \frac{a_n}{n!} z^n$ is an E-function. An E-function is an entire function. The set of E-functions is a ring (for the Cauchy product) which contains the exponential function and the Bessel functions for instance. Its units are of the form $\alpha \exp(\beta z)$, where $\alpha \in \overline{\mathbb{Q}}^*$ and $\beta \in \overline{\mathbb{Q}}$ (André [1]). The set of G-functions is also a ring (for the Cauchy product) which contains the algebraic functions over $\overline{\mathbb{Q}}(z)$ holomorphic at $z = 0$, and the polylogarithmic functions $\sum_{n=1}^{\infty} z^n/n^s$ (s an integer). Its units are the algebraic functions over $\overline{\mathbb{Q}}(z)$ holomorphic at $z = 0$ and taking a non-zero value at $z = 0$ (André [2]).

Let us now define two sets related to these functions.

Definition 2 ([4, 5])**.** (i) $\mathbf{E}$ is the set of all E-values, i.e. values taken at algebraic points by E-functions. It is a ring. Its group of units contains $\overline{\mathbb{Q}}^* \exp(\overline{\mathbb{Q}})$.

(ii) $\mathbf{G}$ is the set of all G-values, i.e values taken at algebraic points by (analytic continuation of) G-functions. It is a ring, which contains the values of the Riemann zeta function at integer points. Its group of units contains $\overline{\mathbb{Q}}^*$ and the Beta values $B(\mathbb{Q}, \mathbb{Q})$ (when defined and non-zero). In particular, it contains all the numbers of the form $\Gamma(a/b)^b$, $a, b \geq 1$ integers.

(Recall that $B(x, y) = \Gamma(x)\Gamma(y)/\Gamma(x+y)$.) Conjecturally, $\mathbf{E} \cap \mathbf{G} = \overline{\mathbb{Q}}$ but so far only the trivial inclusion $\overline{\mathbb{Q}} \subset \mathbf{E} \cap \mathbf{G}$ is known. Still conjecturally, Euler's constant γ and the values $\Gamma(a/b)$, a, b integers with $a/b \notin \mathbb{Z}$, are neither in $\mathbf{E}$ nor in $\mathbf{G}$.

Our works are essentially devoted to the following question: How can the properties of E and G-functions be used to deduce non-trivial properties of the sets $\mathbf{E}$ and $\mathbf{G}$, and vice-versa? In my talk, I mainly focused on E-functions and E-values.

Using the deep properties of the differential equations satisfied by G-functions, in particular certain special basis of solutions at algebraic points (named ACK

basis below, after André, Chudnovsky and Katz), we obtained the following result, which was crucial to prove that **G** is a ring.

Theorem 1 (Fischler-R [4])**.** A number ξ is in **G** if and only if $\xi = F(1)$, where F is a G-function with coefficients in $\mathbb{Q}(i)$, whose radius of convergence can be as large as a priori specified.

In a preliminary version of [4], we asked if something similar could be said for E-values (the statement on the radius being pointless of course). The referee of [4] answered this question in the negative, by means of Beukers' lifting Theorem [3], and an adaptation of his argument shows the following.

Theorem 2. An E-function with coefficients in a number field $\mathbb{K}$ takes at an algebraic point α either a transcendental value or a value in $\mathbb{K}(\alpha)$.

In particular, there is no E-function $F(z) \in \mathbb{Q}[[z]]$ such that $F(1) = \sqrt{2}$.

André's recent theory of E-operators [1] was our starting point to study E-functions and E-values.

Definition 3 (André [1])**.** A differential operator $L \in \overline{\mathbb{Q}}[x, \frac{d}{dx}]$ is an E-operator if the operator $M \in \overline{\mathbb{Q}}[z, \frac{d}{dz}]$ obtained from L by formally changing $x \to -\frac{d}{dz}$ and $\frac{d}{dx} \to z$ (the Fourier-Laplace transform of L) is a G-operator, i.e. $My(z) = 0$ has at least one G-function solution for which it is minimal.

Given an E-function $F(x) = \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n$, there exists an E-operator L, of order μ say, such that $LF(x) = 0$. Moreover, the Laplace transform of $F(x)$, defined by $g(z) = \int_0^{\infty} F(x)e^{-xz}dx = \sum_{n=0}^{\infty} \frac{a_n}{z^{n+1}}$, is a G-function of the variable $1/z$, and $((\frac{d}{dz})^{\mu} \circ M)g(z) = 0$. This connection between E and G-functions enabled André to prove the following.

Theorem 3 (André [1])**.** (i) An E-operator has at most 0 and ∞ as singularities: 0 is always a regular singularity, while ∞ is an irregular one in general. (ii) An E-operator L of order μ has a basis of solutions at $z = 0$ of the form $(E_1(z), \ldots, E_{\mu}(z)) \cdot z^M$ where M is an upper triangular $\mu \times \mu$ matrix with coefficients in $\mathbb{Q}$ and the $E_j(z)$ are E-functions.

Any local solution $F(z)$ of $Ly(z) = 0$ at $z = 0$ is thus of the form

$$F(z) = \sum_{j=1}^{\mu} \Big(\sum_{s \in S_j} \sum_{k \in K_j} \phi_{j,s,k} z^s \log(z)^k \Big) E_j(z)$$

where $S_j \subset \mathbb{Q}, K_j \subset \mathbb{N}$ are finite and $\phi_{j,s,k} \in \mathbb{C}$. We studied in[7] E-operators with trivial monodromy at the origin.

Theorem 4 (R-Roques [7])**.** Consider an E-operator $L \in \overline{\mathbb{Q}}[z, \frac{d}{dz}]$ of order μ having a basis over $\mathbb{C}$ of holomorphic solutions at $z = 0$. Then, L has a basis over $\mathbb{C}$ of solutions of the form $P_1(z)e^{\beta_1 z} + \cdots + P_{\ell}(z)e^{\beta_{\ell} z}$ for some integer $\ell \leq \mu$, some β_j's in $\overline{\mathbb{Q}}^*$, and some $P_j(z)$'s in $\overline{\mathbb{Q}}[z]$.

We now focus on *connection constants*. For G-operators, we proved in [4] that the connection constants are always in $\mathbf{G}$ when we connect an ACK basis at α to an ACK basis at β, where $\alpha, \beta \in \overline{\mathbb{Q}} \cup \{\infty\}$. This property was an important step in the proof of Theorem 1 previously stated. In [5], we also characterized the nature of connection constants of E-operator at finite distance. Now, let $F(z)$ be a local solution of an E-operator $Ly(z) = 0$ at $z = 0$ with $\phi_{j,s,k} \in \overline{\mathbb{Q}}$. Any point $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$ being a regular point of L, there exists a basis of local solutions, holomorphic around $z = \alpha$, $F_1(z-\alpha), \ldots, F_\mu(z-\alpha) \in \overline{\mathbb{Q}}[[z-\alpha]]$ such that $F(z) = \omega_1 F_1(z-\alpha) + \cdots + \omega_\mu F_\mu(z-\alpha)$ where $\omega_1, \ldots, \omega_\mu$ are connection constants.

Theorem 5 (Fischler-R [5])**.** The connection constants $\omega_1, \ldots, \omega_\mu$ belong to $\mathbf{E}[\log \alpha]$, and even to $\mathbf{E}$ if $F(z)$ is an E-function.

I also presented our results concerning the solutions of an E-operator at $z = \infty$. By deformation of the integral $F(x) = \frac{1}{2i\pi} \int_L g(z) e^{zx} dz$ (L "vertical"), we obtained in [5] a new and explicit description of some of André's results, in particular the generalized asymptotic expansion

$$F(z) \sim \sum_{\rho \in \Sigma} e^{\rho z} \sum_{\alpha \in S} z^\alpha \sum_{i \in T} \log(z)^i \sum_{n=0}^{\infty} \frac{n! c_{\theta,\rho,\alpha,i}(n)}{z^n} \tag{1}$$

as $|z| \to \infty$ in an angular sector bisected by $\{z : \arg(z) = \theta\}$. The sets $\Sigma \subset \overline{\mathbb{Q}}$, $S \subset \mathbb{Q}$, $T \subset \mathbb{N}$ are finite, and a priori $c_{\theta,\rho,\alpha,i}(n) \in \mathbb{C}$. This enabled us to obtain an explicit version of André's duality theorem: The series $\sum_{n=0}^{\infty} \frac{n! c_{\theta,\rho,\alpha,i}(n)}{z^n}$ in (1) is divergent, but $\sum_{n=0}^{\infty} \frac{1}{n!} c_{\theta,\rho,\alpha,i}(n) z^n$ is a finite linear combination of E-functions. We also found explicit expressions for André's basis at infinity $H_1(z), \ldots, H_\mu(z)$, which are of formal solutions at infinity of the E-operator L that annihilates $F(z)$. Each H_k involves series like in (1) but with coefficients in $\overline{\mathbb{Q}}$. The asymptotic expansion (1) of $F(z)$ in a sector bisected by $\{z : \arg(z) = \theta\}$ is $\omega_{\theta,1} H_1(z) + \cdots + \omega_{\theta,\mu} H_\mu(z)$ where the Stokes' constants $\omega_{\theta,k}$ may depend on θ (Stokes' phenomenon). Let us define the set $\mathbf{S}$ as the module generated over $\mathbf{G}[\gamma]$ by all the values of the Gamma function at rational points, where γ is Euler's constant.

Theorem 6 (Fischler-R [5])**.** Let $\theta \in [0, 2\pi)$ be a direction not in some explicit finite set. Then: (i) The Stokes constants $\omega_{\theta,k}$ belong to $\mathbf{S}$. (ii) All the coefficients $c_{\theta,\rho,\alpha,i}(n)$ belong to $\mathbf{S}$.

The determination of connection constants or of Stokes' constants for E or G-functions have a Diophantine interest. Indeed, it is important in the proof of Theorem 7 below and to construct in an effective way new sequences of rational or algebraic approximations to E-values, G-values but also to values of the Gamma function at rational points. This may help to find irrationality proving sequences for numbers like $\zeta(5)$ or $\Gamma(1/5)$. In [4], we completely characterized the set of G-approximable numbers, i.e. numbers $\alpha \in \mathbb{C}$ for which there exist two sequences $(P_n)_n$ and $(Q_n)_n$ of algebraic numbers such that $\lim_n \frac{P_n}{Q_n} = \alpha$ and $\sum_{n=0}^{\infty} P_n z^n$

and $\sum_{n=0}^{\infty} Q_n z^n$ are G-functions. This set is $\operatorname{Frac}\mathbf{G}$. We were led to define this notion because of Apéry's famous sequences of approximations of $\zeta(3)$, which are G-approximations. In [5], we defined a similar notion for E-functions.

Definition 4. Sequences $(P_n)_n$ and $(Q_n)_n$ of algebraic numbers are said to form E-approximations of $\alpha \in \mathbb{C}$ if $\lim_n \frac{P_n}{Q_n} = \alpha$ and $\sum_{n=0}^{\infty} P_n z^n = a(z) \cdot E\big(b(z)\big)$, and $\sum_{n=0}^{\infty} Q_n z^n = c(z) \cdot F\big(d(z)\big)$ where E and F are E-functions, and a, b, c, d are algebraic functions in $\overline{\mathbb{Q}}[[z]]$ with $b(0) = d(0) = 0$. The number α is said to be E-approximable.

The notion is more complicated than for G-functions but it is natural because many sequences of algebraic approximations of classical numbers are E-approximations: For instance diagonal Padé approximants to $\exp(z)$ evaluated at z algebraic, and in particular the convergents to e. Given $X, Y \subset \mathbb{C}$, let $X \cdot Y = \{xy \,\big|\, x \in X, y \in Y\}$ and $\frac{X}{Y} = \{\frac{x}{y} \,|\, x \in X, y \in Y \setminus \{0\}\}$.

Theorem 7 (Fischler-R [5])**.** The set of E-approximable numbers contains $\frac{\mathbf{E} \cup \Gamma(\mathbb{Q})}{\mathbf{E} \cup \Gamma(\mathbb{Q})} \cup \operatorname{Frac}\mathbf{G}$ and it is contained in $\frac{\mathbf{E} \cup (\Gamma(\mathbb{Q}) \cdot \mathbf{G})}{\mathbf{E} \cup (\Gamma(\mathbb{Q}) \cdot \mathbf{G})} \cup (\Gamma(\mathbb{Q}) \cdot \exp(\overline{\mathbb{Q}}) \cdot \operatorname{Frac}\mathbf{G})$.

It would be very interesting to close the gap and to obtain a definitive result as for G-approximable numbers. Finally, I presented two results related to the problem of the determination of the group of units $\mathbf{E}^*$ of $\mathbf{E}$. Again, André's theory of E-operators was an important tool.

Theorem 8 (R-Roques [6])**.** Consider two E-functions $f(z), g(z)$ and $M(z) \in M_2(\overline{\mathbb{Q}}(z))$ such that $\begin{pmatrix} f'(z) \\ g'(z) \end{pmatrix} = M(z) \begin{pmatrix} f(z) \\ g(z) \end{pmatrix}$. If $f(z)$ and $g(z)$ are algebraically dependent over $\overline{\mathbb{Q}}(z)$, then one of the following cases occurs:

(i) There exist $a(z), b(z), c(z), d(z) \in \overline{\mathbb{Q}}[z, z^{-1}]$ and $\alpha, \beta \in \overline{\mathbb{Q}}$ such that

$$f(z) = a(z)e^{\alpha z} + b(z)e^{\beta z} \quad \text{and} \quad g(z) = c(z)e^{\alpha z} + d(z)e^{\beta z}.$$

(ii) There exist $a(z), b(z), c(z), d(z) \in \overline{\mathbb{Q}}[z, z^{-1}]$, $\delta \in \mathbb{Q} \setminus \mathbb{Z}$ and $\alpha \in \overline{\mathbb{Q}}$ such that

$$f(z) = a(z)\,{}_1F_1(1; \delta; \alpha z) + b(z) \quad \text{and} \quad g(z) = c(z)\,{}_1F_1(1; \delta; \alpha z) + d(z).$$

Using as a starting point Beukers' lifting Theorem [3], then Theorem 8 above, and finally the classical Siegel-Shidlovsky Theorem [8], we obtained a result towards a proof that $\mathbf{E}^* = \overline{\mathbb{Q}}^* \exp(\overline{\mathbb{Q}})$.

Theorem 9 (R-Roques [6])**.** Let $F(z), G(z)$ be E-functions and $M(z) \in M_2(\overline{\mathbb{Q}}(z))$ such that $\begin{pmatrix} F'(z) \\ G'(z) \end{pmatrix} = M(z) \begin{pmatrix} F(z) \\ G(z) \end{pmatrix}$. Let us assume that $\xi \in \overline{\mathbb{Q}}^*$ is such that $F(\xi)G(\xi) = 1$. Then $F(\xi)$ and $G(\xi)$ are both in $\overline{\mathbb{Q}}^* \exp(\overline{\mathbb{Q}})$.

References

[1] Y. André, *Séries Gevrey de type arithmétique I. Théorèmes de pureté et de dualité*, Annals of Math. **151** (2000), 705–740.

[2] Y. André, *G-functions and geometry*, Aspects of Math. **E13**, Vieweg, 1989.

[3] F. Beukers, *A refined version of the Siegel-Shidlovskii theorem*, Annals of Math. **163** (2006), no. 1, 369–379.
[4] S. Fischler and T. Rivoal, *On the values of G-functions*, Commentarii Math. Helv. **29** (2014), no. 2, 313–341.
[5] S. Fischler and T. Rivoal, *Arithmetic theory of E-operators*, Journal de l'École polytechnique - Mathématiques, 3 (2016), 31–65.
[6] T. Rivoal and J. Roques, *On the algebraic dependence of E-functions*, (2015), 10 pages, to appear in Bull. Lond. Math. Soc.
[7] T. Rivoal and J. Roques, *Holomorphic solutions of E-operators*, preprint (2016), 6 pages.
[8] A. B. Shidlovskii, *Transcendental Numbers*, de Gruyter Studies in Mathematics **12**, 1989.

Tanguy Rivoal, CNRS and Université Grenoble Alpes, CS 40700, 38058 Grenoble cedex 9, France.

Values of Mahler functions and Galois theory

Patrice Philippon

1. Mahler method

Let $q \in \boldsymbol{N}$, $q \geq 2$, a *q-Mahler function* is an element $f(z) \in \overline{\boldsymbol{Q}}((z))$ solution of an equation

$$a_N(z)f(z^{q^N}) + \cdots + a_0(z)f(z) = 0 \ ,$$

where $a_0(z), \ldots, a_N(z) \in \overline{\boldsymbol{Q}}[z]$, $a_0(z)a_N(z) \neq 0$, and $N \in \boldsymbol{N}^\times$ is the *order* of the equation. Equivalently, a q-Mahler function is a component of a vector $\boldsymbol{f}(z) = (f_1(z), \ldots, f_N(z)) \in \overline{\boldsymbol{Q}}((z))^N$ solution to a matrix equation

$$(1) \qquad {}^t\boldsymbol{f}(z) = A(z)\,{}^t\boldsymbol{f}(z^q) \ , \quad A(z) \in \mathrm{Gl}_N(\overline{\boldsymbol{Q}}(z)) \ .$$

The *singular locus* of the system is

$$\left\{\xi \in \overline{\boldsymbol{Q}}^\times ; \exists k \in \boldsymbol{N} \text{ such that } \xi^{q^k} \text{ is a pole of } A(z) \text{ or } A(z)^{-1}\right\} \ .$$

A Mahler function is said to be non singular at α if it satisfies a system (1) the singular locus of which does not contain α. Also, a Mahler function is meromorphic in the non-bordered unit disc, with possible poles at 0 and the singular locus. A common denominator of the components of $\boldsymbol{f}(z)$ outside of 0 is written $\prod_{\xi \in S, \ell \in \boldsymbol{N}} (1 - \xi^{-1} z^{q^\ell})^{m_\xi}$, where S is the set of poles of the coefficients of $A(z)$ and m_ξ is the multiplicity of such a pole ξ.

Theorem 1. (Kumiko Nishioka). Let $\boldsymbol{f}(z)$ be a vector of q-Mahler functions solution to (1) and $\alpha \in \overline{\boldsymbol{Q}}^\times$, $|\alpha| < 1$, which is not a singularity of this system. Then $\mathrm{trdeg}_{\overline{\boldsymbol{Q}}} \overline{\boldsymbol{Q}}(\boldsymbol{f}(\alpha)) = \mathrm{trdeg}_{\overline{\boldsymbol{Q}}(z)} \overline{\boldsymbol{Q}}(z, \boldsymbol{f}(z))$.

Problem - Knowing the transcendence degree does not tell everything about the algebraic relations between the values. For example, $f_1(z)$ may be a transcendental function and nevertheless take algebraic values at some algebraic points. How to determine those points?

In case of functions satisfying Mahler equations of order $N \leq 2$ we can say more.

2. Order one and two

Let K be a number field and $\alpha \in K^\times$, $|\alpha| < 1$. Denote $\mathcal{H}$ the multiplicative group $\left\{\frac{r(z^q)}{r(z)}; r(z) \in K(z)^\times\right\}$ and set

$$\mathcal{R} := \left\{r(z) \in K(z); r(0) = 0 \text{ and } r(\alpha^{q^k}) \neq \infty, \forall k \in \boldsymbol{N}\right\} .$$

Select a collection $\mathcal{S}$ of element of $(1+\mathcal{R}) \cap (1+\mathcal{R})^{-1}$ which are multiplicatively independent modulo $\mathcal{H}$ and denote $\mathcal{A}_{q,\alpha,\mathcal{S}}$ the following set of numbers

$$\left\{\prod_{k\in\boldsymbol{N}} s(\alpha^{q^k}); s \in \mathcal{S}\right\} \bigcup \left\{\sum_{k\in\boldsymbol{N}} s(\alpha)\dots s(\alpha^{q^k}) r(\alpha^{q^k}); r(z) \in \mathcal{R}, s(z) \in \mathcal{S}\right\} .$$

Theorem 2. If $x_1, \dots, x_N \in \mathcal{A}_{q,\alpha,\mathcal{S}}$ are such that $1, x_1, \dots, x_N$ are linearly independent over K, then $x_1, \dots, x_N$ are algebraically independent (over $\overline{\boldsymbol{Q}}$).

Proof. It relies on a theorem of Kenneth Kubota (recently revisited *via* Galois theory by Pierre Nguyen Phu Qui) describing explicitly the algebraic relations between the functions $\prod_{k\in\boldsymbol{N}} s(z^{q^k})$ and $\sum_{k\in\boldsymbol{N}} s(z)\dots s(z^{q^k}) r(z^{q^k})$, which satisfy Mahler equations of order 1 and 2 respectively. □

3. Higher orders

There is no such nice description of the algebraic relations between Mahler functions of higher orders, as Kubota's theorem. In each given case, the ideal of relations may be determined, first computing the Galois group of the equation. But, this is not enough to know the relations between the values of the functions.

Let $\alpha \in \overline{\boldsymbol{Q}}^\times$, $|\alpha| < 1$, and consider a vector of q-Mahler functions given by $\boldsymbol{f}(z) = (f_1(z), \dots, f_N(z))$ solution to an $N \times N$-matrix functional equation (1) not singular at α. Set $\boldsymbol{X} = (X_1, \dots, X_N)$.

Theorem 3. (Main theorem). If $P \in \overline{\boldsymbol{Q}}[\boldsymbol{X}]$ satisfies $P(\boldsymbol{f}(\alpha)) = 0$, then there exists $Q \in \overline{\boldsymbol{Q}}[z, \boldsymbol{X}]$ such that $Q(z, \boldsymbol{f}(z)) \equiv 0$, $\mathrm{d}^\circ_{\boldsymbol{X}} Q = \mathrm{d}^\circ P$ and $P(\boldsymbol{X}) = Q(\alpha, \boldsymbol{X})$.

This is the analogue for Mahler functions of a result of Frits Beukers for E-functions. Knowing the algebraic relations between the functions, the Main theorem gives those between their values at non singular arguments.

Restricting the entries of the matrix $A(z)$ to have coefficients in a given number field K, we can speak of (q, K)-Mahler functions. Define the K-vector space

$$\mathcal{V}_{q,\alpha}(K) := \{f(\alpha); f \text{ a } (q, K)\text{-Mahler function not singular at } \alpha\} .$$

Corollary 1. Let $x_1, \dots, x_N \in \mathcal{V}_{q,\alpha}(K)$ which are linearly independent over K, then they are linearly independent over $\overline{\boldsymbol{Q}}$.

This may be seen as an analogue of Baker's theorem for values of (q, K)-Mahler functions (instead of logarithms of algebraic numbers).

Example? - Let $b, q \in \boldsymbol{N}$, $b, q \geq 2$, (q, b)-*automatic numbers* are real numbers the sequences of digits in base b of which are given by q-automata. However, they may not all belong to $\mathcal{V}_{q,\frac{1}{b}}(\boldsymbol{Q})$ since $\frac{1}{b}$ may be a singularity of the Mahler equation associated to the generating series of the sequence of digits.

Nevertheless, in 1968 Alan Cobham conjectured that an automatic number is either rational or transcendental. Proving this conjecture *via* Mahler's method could be called "Alf's dream", since Alf van der Poorten together with John Loxton studied the question steadily from 1980 on. But, because of the above snag, even our Main theorem seems to miss this application. Fortunately, Boris Adamczewski and Yann Bugeaud proved Cobham's conjecture in 2007 ... using Wolfgang Schmidt's subspace theorem.

4. Chasing singularities

Here is another way out, repelling the singularities towards the unit circle. But before, I want to mention that Boris Adamczewski and Colin Faverjon had devised another method of "desingularization" before I came out with the following lemma.

Lemma 1. Assume that the matrix $A(z)$ has its coefficients in $K[z]$ and that the numbers $f_{i_1}(\alpha), \ldots, f_{i_\ell}(\alpha)$ are linearly independent over K. Then there exists an $N \times N$-matrix $B(z)$ with coefficients in $K[z]$ and a vector $\boldsymbol{g}(z)$ solution to ${}^t\boldsymbol{g}(z) = B(z){}^t\boldsymbol{g}(z^q)$, such that $\det(B(\alpha^{q^k})) \neq 0$ for $k \in \boldsymbol{N}$ and $Kf_{i_1}(\alpha) + \cdots + Kf_{i_\ell}(\alpha) = Kg_{i_1}(\alpha) + \cdots + Kg_{i_\ell}(\alpha)$.

This, together with a reduction of Jason Bell, Yann Bugeaud and Michael Coons (also revisited by Adamczewski and Faverjon), extends the corollary to our Main theorem to the larger class of numbers:

$$\mathcal{W}_{q,\alpha}(K) := \{f(\alpha); f \text{ a } (q, K)\text{-Mahler function defined at } \alpha\} \ .$$

Thus, we eventually get a proof of Cobham's conjecture *via* Mahler's method, extending the result of Adamczewski and Bugeaud on one hand to β-expansions with $\beta > 1$ any real algebraic number and on the other hand to linear independence (over $\overline{\boldsymbol{Q}}$).

Furthermore, Adamczewski and Faverjon have obtained a complete description of the linear relations between elements of $\mathcal{W}_{q,\alpha}(K)$ subject to a mild restriction.

Theorem 4. (Boris Adamczewski & Colin Faverjon). Let $\boldsymbol{f}(z) = (f_1(z), ..., f_n(z))$ be a vector of (q, K)-Mahler functions, solution to (1). Let $\alpha \in K$, $0 < |\alpha| < 1$, there exists an integer ℓ such that if α is not a pole of $A_\ell(z) := A(z)A(z^q)...A(z^{q^{\ell-1}})$ then

$$\boldsymbol{f}(\alpha)^{\perp\overline{\boldsymbol{Q}}} = \left(\ker_K(A_\ell(\alpha)) + (\boldsymbol{f}(z)^{\perp_{K(z)}})(\alpha)\right) \otimes_K \overline{\boldsymbol{Q}} \ .$$

Here $\boldsymbol{f}(\alpha)^{\perp_{\overline{\boldsymbol{Q}}}}$ is the $\overline{\boldsymbol{Q}}$-vector subspace of $\overline{\boldsymbol{Q}}^N$ orthogonal to $\boldsymbol{f}(\alpha)$ in $\boldsymbol{C}^N$, $\boldsymbol{f}(z)^{\perp_{K(z)}}$ is the $K(z)$-vector subspace of $K(z)^N$ orthogonal to $\boldsymbol{f}(z)$ in $K((z))^N$ and $\ker_K(A_\ell(\alpha))$ is the left kernel in K^N of the matrix $A_\ell(\alpha)$.

In order to go further, one would like to have a description of the Galois group of a Mahler system of functional equations in terms of the matrix of the system ... another dream.

References

[1] B.Adamczewski & C.Faverjon – *Méthode de Mahler : relations linéaires, transcendance et applications aux nombres automatiques*, `arXiv:1508.07158`.

[2] P.Philippon – *Groupes de Galois et nombres automatiques*, J. London Math. Soc. (2) **92** (2015), 596–614.

Diophantine approximation of Mahler numbers

Jason Bell

(joint work with Yann Bugeaud and Michael Coons)

Mahler's method is a method in transcendence theory whereby one uses a function $F(x) \in \mathbb{Q}[[x]]$ that satisfies a functional equation of the form

$$\sum_{i=0}^{d} a_i(x) F(x^{k^i}) = 0 \tag{1}$$

for some integers $k \geq 2$ and $d \geq 1$ and polynomials $a_0(x), \ldots, a_d(x) \in \mathbb{Z}[x]$ with $a_0(x)a_d(x) \neq 0$, to give results about the nature of the numbers $F(1/b)$ with $b \geq 2$ an integer such that $1/b$ is in the radius of convergence of $F(x)$. We refer to such numbers $F(1/b)$ as *Mahler numbers*. It is well-known that automatic numbers, numbers whose base-b expansion can be generated by a finite-state automaton for some $b \geq 2$, form a subset of Mahler numbers.

Let ξ be a real number. The *irrationality exponent*, $\mu(\xi)$, of ξ is defined to be the supremum of the set of real numbers μ such that the inequality

$$0 < \left| \xi - \frac{p}{q} \right| < \frac{1}{q^\mu}$$

has infinitely many solutions $(p, q) \in \mathbb{Z} \times \mathbb{N}$. Computing the irrationality exponent of a given real number is generally very difficult, although there are several classes of numbers for which irrationality exponents are well-understood. All rational numbers have irrationality exponent one, and a celebrated theorem of Roth gives that all irrational algebraic numbers have irrationality exponent precisely two. In fact, the set of real numbers with irrationality exponent strictly greater than two has Lebesgue measure zero. Roth's theorem built on work of Liouville, who showed that if ξ is an algebraic number of degree d over $\mathbb{Q}$, then $\mu(\xi) \leq d$. Using this fact, Liouville produced the first examples of transcendental numbers

by constructing real numbers with infinite irrationality exponent; numbers with infinite irrationality exponent are now called *Liouville numbers* in his honour.

Towards classifying irrationality exponents of automatic numbers, Adamczewski and Cassaigne [2] proved that a Liouville number cannot be generated by a finite-state automaton.

In our work, we use Mahler's method to provide the following generalisation of Adamczewski and Cassaigne's result.

Theorem 1. A Mahler number cannot be a Liouville number.

Historically, the application of Mahler's method had one major impediment. In order to consider numbers $F(1/b)$ one must ensure that $a_0((1/b)^{k^i}) \neq 0$ for all $i \geq 0$; this condition is commonly referred to as *Mahler's condition*. Note that in the statement of Theorem 1 no such condition is stated. Indeed, we are able to remove Mahler's condition within the setting of our paper.

In fact a general quantitative version of Theorem 1 is proved in our work, in which we give a bound for the irrationality exponent of the number $F(a/b)$ in terms of information from the functional equation (1) and the rational number a/b when $|a|$ is small enough compared to b. Indeed, the rational approximations constructed to get the quantitative bound are of high enough quality that we may apply a p-adic version of Schmidt's subspace theorem to extend a result of Adamczewski and Bugeaud [1] on transcendence of automatic numbers to a much larger class of Mahler numbers.

To explain this extension formally, let $\mathbf{a} = \{a(n)\}_{n\geq 0}$ be a sequence taking values in a field $\mathbb{K}$. We define the k-kernel of $\mathbf{a}$, denoted by $\mathcal{K}_k(\mathbf{a})$, as the set of distinct subsequences of the form $\{a(k^\ell n + r)\}_{n\geq 0}$ with $\ell \geq 0$ and $0 \leq r < k^\ell$. Christol showed that a sequence is k-automatic if and only if its k-kernel is finite. We say the sequence $\mathbf{a}$ is *k-regular* (or just *regular*) provided the $\mathbb{K}$-vector space spanned by $\mathcal{K}_k(\mathbf{a})$ is finite-dimensional. We use the term *regular number* to refer the values of a the generating function of a k-regular sequence at rationals $1/b$, with $b \geq 2$ an integer. We then have the following result on transcendence.

Theorem 2. An irrational regular number is transcendental.

As an immediate corollary of this result, we have that if $F(x)$ is a Mahler function satisfying (1) with $a_0(x)$ a non-zero integer, then $F(1/b)$ is either rational or transcendental.

Mahler introduced two related measures of the quality of approximation of a complex transcendental number ξ by algebraic numbers. For any integer $m \geq 1$, we let $w_m(\xi)$ denote the supremum of the real numbers w for which

$$0 < |P(\xi)| < \frac{1}{H(P)^w}$$

has infinitely many solutions in integer polynomials $P(x)$ of degree at most m, where $H(P)$ is the naïve height of the polynomial $P(x)$; that is, it is the maximum

of the absolute values of its coefficients. Further, we set

$$w(\xi) = \limsup_{m\to\infty} \frac{w_m(\xi)}{m}.$$

Following Mahler, we say that ξ is an

- S-number, if $w(\xi) < \infty$;
- T-number, if $w(\xi) = \infty$ and $w_m(\xi) < \infty$ for any integer $m \geq 1$;
- U-number, if $w(\xi) = \infty$ and $w_m(\xi) = \infty$ for some integer $m \geq 1$.

Almost all numbers are S-numbers in the sense of Lebesgue measure, and Liouville numbers are examples of U-numbers. Then according to this taxonomy, we have the following result.

Theorem 3. An irrational regular number is an S-number or a T-number.

Since automatic numbers form a subset of regular numbers, Theorem 3 implies that any irrational automatic number is either an S-number or a T-number.

References

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

[2] B. Adamczewski and J. Cassaigne, *Diophantine properties of real numbers generated by finite automata*, Compos. Math. **142**(6) (2006), 1351–1372.

Measures of algebraic independence and Diophantine properties of Mahler numbers and their generalizations.

Evgeniy Zorin

This report presents some new measures of algebraic independence for values of Mahler functions and their generalizations. Among the other things, we provide a result on a measure of algebraic independence at transcendental points, see Theorem 3 below. We also show how these results imply that no Mahler number belongs to the class U in Mahler's classification (see Corollary 1 below).

So, let $n \in \mathbb{N}$ and let $p(\underline{z}) = p_1(\underline{z})/p_2(\underline{z})$ be a rational function with coefficients in $\overline{\mathbb{Q}}$. *Mahler functions* is a system of functions

$$f_1(\underline{z}), ..., f_n(\underline{z}) \in \overline{\mathbb{Q}}[[\underline{z}]]$$

analytic in some neighbourhood U of 0 and satisfying the following system of functional equations:

$$a(\underline{z})\underline{f}(\underline{z}) = A(\underline{z})\underline{f}(p(\underline{z})) + B(\underline{z}), \tag{1}$$

where $\underline{f}(\underline{z}) = (f_1(\underline{z}), \ldots, f_n(\underline{z}))$, $a(\underline{z}) \in \overline{\mathbb{Q}}[\underline{z}]$, A (resp. B) is an $n \times n$ (resp. $n \times 1$) matrix with coefficients in $\overline{\mathbb{Q}}[\underline{z}]$ and we assume that the order of vanishing of $p(z)$ at 0 is at least 2, that is $\mathrm{ord}_{\underline{z}=0} p := \mathrm{ord}_{\underline{z}=0} p_1 - \mathrm{ord}_{\underline{z}=0} p_2 \geq 2$. We will denote by d the degree of $p(z)$ (i.e. $d = \max(\deg p_1(z), \deg p_2(z))$) and by δ the order of vanishing of $p(z)$ at $z = 0$.

We denote by t the transcendence degree

$$t := \mathrm{tr.deg.}_{\mathbb{C}(z)}\mathbb{C}(f_1(z),\dots,f_n(z)), \tag{2}$$

that is t is the maximal number of functions among $f_1(z),\dots,f_n(z)$ which are algebraically independent over $\mathbb{C}(z)$. We will denote by $I_{\underline{f}} \subset \overline{\mathbb{Q}}[z][X_1,\dots,X_n]$ the ideal of polynomials that vanish on $f_1(z),\dots,f_n(z)$.

For a variety $W \subset \mathbb{P}^n$ one can define the notions of *height* and *degree*, generalizing the corresponding notions for a polynomial. These definitions and a detailed discussion of them can be found, for example, in Chapters 5 and 7 of [2]. To get a flavour of (most of) the statements presented in this report it might be enough to keep in mind the case when the variety W is a lieu of zeros of a homogeneous (in $X_1,\dots,X_n$) polynomial $P \in \mathbb{Z}[z][X_1,\dots,X_n]$. In this case, the height of W, $h(W)$, equals to the logarithmic Weil height of P and the degree of W, $\deg(W)$, equals to the degree of W. Similarly, in this case the projective distance $\mathrm{Dist}(x,W)$ can be substituted by the normalized value of polynomial P at x, that is $\frac{|P(x')|}{|P|\cdot|x'|^{\deg P}}$, where x' stands for any representative of the projective point x, $|P(x')|$ denotes the absolute value of $P(x')$ (archimedean or not), $|P|$ denotes the maximum of absolute values of coefficients of P and $|x'|$ is the maximum of absolute values of coordinates of x'.

Our first two theorems give the measure of algebraic independence of Mahler functions at algebraic points.

Theorem 1. Let $p(z) \in \overline{\mathbb{Q}}[z]$ and let $f_1(z),\dots,f_n(z)$ be functions analytic in a neighbourhood U of the origin and satisfying (1). Let $y \in \overline{\mathbb{Q}} \cap U$ verifies

$$p^{[h]}(y) \to 0$$

as $h \to \infty$ and no iterate $p^{[h]}(y)$ is a zero of $z \det A(z)$.

Then there is a constant $C > 0$ such that for any variety $W \subset \mathbb{P}^n_{\overline{\mathbb{Q}}}$ of dimension $k < t + 1 - \frac{\log d}{\log \delta}$, one has

$$\log \mathrm{Dist}(x,W) \geq -Ch(W)\,(\log h(W))^{\frac{(t+1)\left(\frac{\log d}{\log\delta}-1\right)}{t-k+1-\frac{\log d}{\log\delta}}}\,(\deg(W))^{\frac{t+1}{t-k+1-\frac{\log d}{\log\delta}}}, \tag{3}$$

where $x = (1 : f_1(y) : \dots : f_n(y)) \in \mathbb{P}^n_{\mathbb{C}}$.
In particular,

$$\mathrm{tr.deg.}_{\mathbb{Q}}\mathbb{Q}\,(f_1(y),\dots,f_n(y)) \geq t + 1 - \left\lfloor \frac{\log d}{\log \delta} \right\rfloor,$$

and if we assume moreover $\frac{\log d}{\log \delta} < 2$ then

$$\mathrm{tr.deg.}_{\mathbb{Q}}\mathbb{Q}\,(f_1(y),\dots,f_n(y)) = t.$$

Theorem 2. Let $f_1(z),\dots,f_n(z)$ be a collection of functions analytic in a neighbourhood U of the origin and satisfying (1). In this statement we assume $\underline{p}(\underline{z}) \in \overline{\mathbb{Q}}(\underline{z})$ in the system (1) (compare with more restrictive assumption $p(\underline{z}) \in \overline{\mathbb{Q}}[\underline{z}]$ in the preceding Theorem 1). We keep the notation $d = \deg p$, $\delta = \mathrm{ord}_{\underline{Z}=0}p \geq 2$. Assume that a number $y \in \overline{\mathbb{Q}} \cap U$ satisfies $\lim_{h\to\infty} p^{[h]}(y) = 0$ and for all $h \in \mathbb{N}$

the number $p^{[h]}(y)$ is not a zero of $z \det A(\underline{z})$. Then there is a constant $C > 0$ such that for any variety $W \subset \mathbb{P}^n_{\mathbb{Q}}$ of dimension $k < t\left(2 - \frac{\log d}{\log \delta}\right)$, one has

$$\log \mathrm{Dist}(\underline{x}, W) \geq -Ch(W)^{1+\frac{\log d - \log \delta}{(2t-k)\log \delta - t \log d} t} \deg(W)^{\frac{2t}{t\left(2-\frac{\log d}{\log \delta}\right)-k}}, \tag{4}$$

where $\underline{x} = (1 : f_1(y) : \cdots : f_n(y)) \in \mathbb{P}^n_{\mathbb{C}}$. In particular,

$$\mathrm{tr.deg.}_{\mathbb{Q}} \mathbb{Q}\left(f_1(y), \ldots, f_n(y)\right) \geq t\left(2 - \frac{\log d}{\log \delta}\right). \tag{5}$$

Also, it is possible to give a measure of algebraic independence for values of Mahler functions at arbitrary complex value of argument. Note that in the statement of Theorem 3 below we does not assume $y \in \overline{\mathbb{Q}}$ (though in this case we have significantly less sharp estimates, if compared to our Theorems 1 and 2 above, where we assume that y is algebraic).

Theorem 3. Let $f_1(z),\ldots,f_n(z)$ be functions analytic in a neighbourhood U of the origin and satisfying (1). Assume that $p(z) \in \overline{\mathbb{Q}}[z]$ with $\delta = \mathrm{ord}_{z=0}\, p(z) \geq 2$ and $d = \deg p(z)$. Let $y \in U$ be such that

$$p^{[h]}(y) \to 0 \text{ as } h \to \infty$$

and no iterate $p^{[h]}(y)$ is a zero of $z \det A(z)$.

Then for all $\varepsilon > 0$ there is a constant C such that for any variety $W \subset \mathbb{P}^{n+1}_{\mathbb{Q}}$ of dimension $k < t + 1 - 2\frac{\log d}{\log \delta}$, one has

$$\log \mathrm{Dist}(x, W) \geq -C \max\left((\deg(W))^{\frac{t+2+\varepsilon}{t-k+1-2\frac{\log d}{\log \delta}-\varepsilon}}, h(W)^{\frac{t+2+\varepsilon}{t-k+2-\frac{\log d}{\log \delta}-\varepsilon}} \right), \tag{6}$$

where $x = (1 : y : f_1(y) : \cdots : f_n(y)) \in \mathbb{P}^{n+1}_{\mathbb{C}}$.
In particular,

$$\mathrm{tr.deg.}_{\mathbb{Q}} \mathbb{Q}\left(y, f_1(y), \ldots, f_n(y)\right) \geq t + 1 - \left[2\frac{\log d}{\log \delta}\right],$$

and if we assume moreover $\frac{\log d}{\log \delta} < 3/2$ then

$$\mathrm{tr.deg.}_{\mathbb{Q}} \mathbb{Q}\left(y, f_1(y), \ldots, f_n(y)\right) \geq t - 1.$$

The proof of all these results exploits new general multiplicity estimate [3], which gives, in particular, an essentially optimal (up to a multiplicative constant) multiplicity estimate for Mahler functions

If the rational function $p(z)$ satisfies the condition $\deg p(z) = \mathrm{ord}_{\underline{z}=0} p(z)$, then lower bounds (3) and (4) are the best possible in terms of the dependence on the (logarithmic Weil) height, $h(W)$. In this case, by applying Theorem 1 to (1) with the function $p(z) = z^d$ and the variety W_P equal to the lieu of common zeros of an ideal $I_{\underline{f}}$ and an arbitrary polynomial $P \in \mathbb{Z}[X_1]$, we find the following corollary:

Corollary 1. Let $p(z) = z^d$ and let $f_1(z), \ldots, f_n(z)$ be a solution to the system (1) analytic in a neighbourhood of zero. Let $\alpha \in \overline{\mathbb{Q}}$ verifies $0 < |\alpha| < 1$.

Then the number $f_1(\alpha)$ is not a U-number.

More precisely, one of the following two complimentary options holds true

(1) $f_1(z) \in \overline{\mathbb{Q}}(z)$, and then $f_1(\alpha)$ is an algebraic number, hence not in the class U.

(2) $f_1(z) \notin \overline{\mathbb{Q}}(z)$, and then there exist constants $C_3, T > 0$ such that for all non-zero $P \in \mathbb{Z}[X]$ we have

$$|P(f_1(\alpha))| \geq \exp\left(-C_3 \left(h(P) + 1\right) \deg(P)^T\right).$$

Corollary 1 follows from Theorem 1, the only point which needs special treatment is the removal of Mahler's condition, that is the hypothesis of Theorem 1 that no iterate $p^{[h]}(y)$, $h \in \mathbb{Z}_{\geq 0}$, of the point $y \in \overline{\mathbb{Q}} \cap U$ is a zero of the polynomial $z \det A(z)$. This can be done with a new method presented in [1, Section 5].

It seems that Corollary 1 could be generalized further, covering not only the classical case of system (1) with $p(z) = z^d$, but also system (1) with any rational function $p(z) \in \overline{\mathbb{Q}}(z)$ verifying $\deg p = \mathrm{ord}_{z=0} p \geq 2$, e.g. $\frac{z^2}{1+z^2}$. The only problem is that in this more general case we lack, at least currently, a structure theorem for the analytic solutions of (1) to use in place of Dumas' theorem in [1, Section 5]. This problem is still to be investigated.

We can still infer from Theorem 2 a conditional result, depending on Mahler's condition.

Corollary 2. Let $p(z) \in \overline{\mathbb{Q}}(z)$ verifies $\deg p(z) = \mathrm{ord}_{z=0} p(z)$ and let $f_1(z), ..., f_n(z)$ be a solution to the system (1) analytic in a neighbourhood U of the origin. Let $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$ verifies

$$p^{[h]}(\alpha) \to 0$$

as $h \to \infty$.

Moreover, assume that no iterate $p^{[h]}(\alpha)$, $h \in \mathbb{Z}_{\geq 0}$, is a zero of $z \det A(z)$ (Mahler's condition).

Then the number $f_1(\alpha)$ is not a U-number.

More precisely, one of the following two complimentary options holds true:

(1) $f_1(\alpha) \in \overline{\mathbb{Q}}$, hence not in the class U.

(2) $f_1(\alpha) \notin \overline{\mathbb{Q}}$, then there exists a constant $C_3 > 0$ such that for all non-zero $P \in \mathbb{Z}[X]$ we have

$$|P(f_1(\alpha))| \geq \exp\left(-C_3 \left(h(P) \deg(P)^{2t} + \deg(P)^{2t+1}\right)\right).$$

References

[1] J. Bell, Y. Bugeaud, M. Coons, "Diophantine approximation of Mahler numbers", Proc. London Math. Soc. (2015) 110 (5): 1157-1206, doi: 10.1112/plms/pdv016

[2] Yu. Nesterenko, P. Philippon (eds.), "Introduction to Algebraic Independence Theory", Vol. 1752, 2001, Springer.

[3] E. Zorin, "Multiplicity Estimates for Algebraically Dependent Analytic Functions", Proceedings of the London Mathematical Society, Vol. 108, No. 4, 04.2014, p. 989–1029.

New Positivity Results for Canonical Heights on Abelian Varieties and an Application to Arithmetic Dynamics

Joseph H. Silverman
(joint work with Shu Kawaguchi)

Canonical Heights for Nef Divisors on Abelian Varieties. Let K be a number field, let X/K a smooth projective variety, and for each irreducible divisor $D \in \mathrm{Div}(X)$, fix a Weil height function

$$h_{X,D} : X(\bar{K}) \longrightarrow \mathbb{R}.$$

Then for $\mathbb{R}$-linear combinations of irreducible divisors $D = \sum c_i D_i \in \mathrm{Div}(X) \otimes \mathbb{R}$, define $h_{X,D}$ by linearity to equal $\sum c_i h_{X,D_i}$.

When X is an abelian variety, the quadratic part of the canonical height is the limit

$$\hat{q}_{X,D} : X(\bar{K}) \longrightarrow \mathbb{R}, \quad \hat{q}_{X,D}(P) = \lim_{n\to\infty} 4^{-n} h_{X,D}(2^n P).$$

We recall some basic facts ([2, 5]):

- The function $\hat{q}_{X,D}$ is a quadratic form.
- The function $\hat{q}_{X,D}$ depends only on the algebraic equivalence class of D in $\mathrm{NS}(X) \otimes \mathbb{R}$.
- If D is ample, then $\hat{q}_{X,D}$ extends to a positive definite quadratic form

$$\hat{q}_{X,D} : X(\bar{K}) \otimes \mathbb{R} \longrightarrow \mathbb{R}.$$

The positivity has many important consequences, including in particular implying that if $P_1, \ldots, P_r$ is a basis for the Mordell–Weil group $X(K)/X(K)_{\mathrm{tors}}$, then the regulator $\det\big(\langle P_i, P_j\rangle\big)$ computed using the associated bilinear form is strictly positive.

The ample cone in $\mathrm{NS}(X) \otimes \mathbb{R}$ is the cone generated by all positive real multiples of ample divisors (together with 0). Then one way to define the *nef cone* in $\mathrm{NS}(X) \otimes \mathbb{R}$ is as the real closure of the ample cone. The abbreviation nef stands for *numerically effective*, since an alternative characterization is that a divisor class $D \in \mathrm{NS}(X) \otimes \mathbb{R}$ is nef if and only if $D \cdot C \ge 0$ for every irreducible curve $C \subset X$. One may thus view nef divisors as limits of ample divisors.

Our main theorem generalizes the positivity of the canonical height for ample divisors to the case that D is nef.

Theorem 1. [4] Let X/K be an abelian variety defined over a number field, and let $D \in \mathrm{NS}(X) \otimes \mathbb{R}$ be a non-zero nef divisor class. Then there is a proper abelian subvariety $Y_D \subsetneq X$ so that for all $P \in X(\bar{K}) \otimes \mathbb{R}$,

$$\hat{q}_{X,D}(P) = 0 \quad \Longleftrightarrow \quad P \in Y_D(\bar{K}) \otimes \mathbb{R}.$$

Of course, if D is ample, then $Y_D = 0$ and we recover the usual result that $P \in X(\bar{K})$ satisfies $\hat{q}_{X,D}(P) = 0$ if and only if $P \in X(\bar{K})_{\mathrm{tors}}$.

The proof of Theorem 1 starts with the identification of $\mathrm{NS}(X) \otimes \mathbb{R}$ as the Jordan algebra of elements in $\mathrm{End}(X) \otimes \mathbb{R}$ fixed by the Rosati involution. It then

uses a theorem stating that the image of the nef cone consists of the positive semi-definite elements in $\mathrm{End}(X) \otimes \mathbb{R}$, where $\mathrm{End}(X) \otimes \mathbb{R}$ is identified with a product of matrix algebras having real, complex, and quaternionic entries. The following transfer formulas for canonical heights also provide a key tool in the proofs.[1]

Proposition 1 (Bertrand Transfer Formulas [1, Proposition 3])**.** Let H be an ample divisor that is used to define the embedding $\mathrm{NS}(X) \otimes \mathbb{R} \hookrightarrow \mathrm{End}(X) \otimes \mathbb{R}$ and let $\alpha \to \alpha'$ denote the associated Rosati involution of $\mathrm{End}(X) \otimes \mathbb{R}$.

(a) For all $P, Q \in A$ and all $\alpha \in \mathrm{End}(X) \otimes \mathbb{R}$, we have

$$\langle \alpha(P), Q \rangle_H = \langle P, \alpha'(Q) \rangle_H.$$

(b) For all $P, Q \in A$ and all $D \in \mathrm{NS}(X) \otimes \mathbb{R}$, we have

$$\langle P, Q \rangle_D = \langle P, \Phi_D(Q) \rangle_H.$$

An Application to Arithmetic Dynamics. Let X be a smooth projective variety, let $f : X \to X$ be a dominant self-morphism[2] of X, and let H be an ample divisor on X, with everything defined over a number field K. The *dynamical degree of* f, which is a measure of the geometric complexity of the iterates of f, is the quantity

$$\delta(f) = \lim_{n\to\infty} \Big(\big((f^n)^* H \big) \cdot H^{\dim(X)-1} \Big)^{1/n}.$$

For example, if $f : \mathbb{P}^N \to \mathbb{P}^N$, then $\delta(f) = \deg(f)$. Analogously, for a point $P \in X(\bar{K})$, the *f-arithmetic degree of* P is the quantity

$$\alpha(f, P) = \lim_{n\to\infty} \Big(h_{X,H}\big(f^n(P)\big) \Big)^{1/n}.$$

Theorem 2. [3, 4] Let $f : X \to X$ be a dominant self-morphism of a smooth projective variety, and let $P \in X(\bar{K})$.

(a) The limit defining $\alpha(f, P)$ exists and is independent of the choice of the ample height function $h_{X,H}$.
(b) The arithmetic degree $\alpha(f, P)$ is an algebraic integer.
(c) The set of arithmetic degrees $\big\{\alpha(f, Q) : Q \in X(\bar{K})\big\}$ is finite.
(d) The arithmetic degree is never larger than the dynamical degree:

$$\alpha(f, P) \le \delta(f).$$

Conjecture 1. [3, 6] With notation as in Theorem 2, let

$$\mathcal{O}_f(P) = \big\{ f^n(P) : n \ge 0 \big\}$$

denote the f-orbit of P. If $\mathcal{O}_f(P)$ is Zariski dense in X, then $\alpha(f, P) = \delta(f)$, i.e., Zariski density of the orbit implies maximality of the arithmetic degree.

We use Theorem 1 to prove Conjecture 1 for abelian varieties. (An analogous result for endomorphisms of algebraic tori is proven in [6].)

[1] It was at this Oberwolfach worksop that the second author learned that he and Kawaguchi had independently rediscovered Bertrand's beautiful formulas.

[2] There are interesting (conjectural) generalizations of the results in this section to dominant *rational* maps $f : X \dashrightarrow X$, but lack of space precludes our discussing them.

Theorem 3. [4, 7] Let $f : X \to X$ be a dominant self-morphism of an abelian variety, everything defined over a number field. Then Conjecture 1 is true, i.e.,

$$\overline{\mathcal{O}_f(P)} = X \quad \Longrightarrow \quad \alpha(f,P) = \delta(f).$$

The proof of Theorem 3 starts by using a fixed point theorem of Birkhoff to construct a non-zero nef divisor class $D_f \in \mathrm{NS}(X) \otimes \mathbb{R}$ having the property that $f^*D_f = \delta(f)D_f$. We then use the abelian subvariety Y_{D_f} constructed in Theorem 1 and prove the chain of implications

$$\alpha(f,P) < \delta(f) \quad \Longrightarrow \quad \hat{q}_{D_f}(P) = 0 \quad \Longrightarrow \quad \mathcal{O}_f(P) \subset Y_{D_f} + X_{\mathrm{tors}},$$

from which a short additional argument gives $\overline{\mathcal{O}_f(P)} \subsetneq X$.

References

[1] Daniel Bertrand, Minimal heights and polarizations on group varieties, *Duke Math. J.* **80** (1995), 223–250.

[2] Marc Hindry and Joseph Silverman, *Diophantine Geometry: An Introduction*, GTM 201, Spring-Verlag, New York, 2000.

[3] Shu Kawaguchi and Joseph Silverman, On the dynamical degree and the arithmetic degree of rational self-maps of algebraic varieties, *J. Reine Angew. Math.*, to appear. `arxiv.1208.0815`.

[4] Shu Kawaguchi and Joseph Silverman, Dynamical canonical heights for Jordan blocks, arithmetic degrees of orbits, and nef canonical heights on abelian varieties, *Trans. AMS*, to appear. `arXiv:1301.4964`.

[5] Serge Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983.

[6] Joseph Silverman, Dynamical degree, arithmetic entropy, and canonical heights for dominant rational self-maps of projective space, *Ergodic Th. and Dyn. Sys.* **34** (2014), 633–664.

[7] Joseph Silverman, Arithmetic and dynamical degrees on abelian varieties, *Journal de Théorie des Nombres de Bordeaux*, to appear. `arXiv:1501.04205`

Lower bound for the Néron-Tate height

Éric Gaudron

(joint work with Vincent Bosser)

We propose a totally explicit lower bound for the Néron-Tate height of algebraic points of infinite order of abelian varieties.

Let k be a number field of degree $D = [k : \mathbb{Q}]$. Let A be an abelian variety defined over a fixed subfield of k, of dimension g. Let L be a polarization of A. We denote by $\widehat{h}_L$ the Néron-Tate height on $A(k)$ relative to L. It is well-known that, for $p \in A(k)$, we have $\widehat{h}_L(p) = 0$ if and only if p is a torsion point, i.e. $np = 0$ for some positive integer n. The general problem of bounding from below $\widehat{h}_L(p)$ when $p \in A(k)$ is not a torsion point has been often tackled in the literature, overall from the point of view of the dependence on D (Lehmer's problem) or on the Faltings height $h_F(A)$ of A (Lang-Silverman conjecture). Moreover most of results concern elliptic curves or abelian varieties with complex multiplication. Let us cite two emblematic results due to David Masser, valid in great generality (A_{tors} is the set of torsion points) [3, 4].

Theorem 1. (Masser, 1985-86). In the above setting, there exist positive constants $c(A,\varepsilon)$ and $c(k,g)$, depending only on A,ε and on k,g respectively, such that, for all $\varepsilon>0$ and all $p\in A(k)\setminus A_{\mathrm{tors}}$, one has

$$\widehat{h}_L(p)^{-1}\le c(A,\varepsilon)D^{2g+1+\varepsilon}\quad\text{and}\quad\widehat{h}_L(p)^{-1}\le c(k,g)\max\left(1,h_F(A)\right)^{2g+1}.$$

Unfortunately, there is no bound which takes into account both degree and Faltings height (at this level of generality). Up to now, there is only one published bound for $\widehat{h}_L(p)^{-1}$ which is totally explicit in all parameters. It is due to Bruno Winckler (PhD thesis, 2015, [8]) valid for a CM elliptic curve A. His bound looks like Dobrowolski-Laurent's one: $c(A)D(\max(1,\log D)/\max(1,\log\log D))^3$ with a constant $c(A)$ quite complicated (but explicit). We propose here the following much simpler bound.

Theorem 2. Let (A,L) be a polarized abelian variety over k and $p\in A(k)\setminus A_{\mathrm{tors}}$. Then we have

$$\widehat{h}_L(p)^{-1}\le\max\left(D+g^g,h_F(A)\right)^{10^5 g}.$$

Note that the bound does not depend on the polarization L. The proof of this theorem involves two ingredients, namely a generalized period theorem and Minkowski's convex body theorem.

Let us explain the first one. Let $\sigma\colon k\hookrightarrow\mathbb{C}$ be a complex embedding. By extending the scalars we get a complex abelian variety $A_\sigma=A\times_\sigma\operatorname{Spec}\mathbb{C}$ isomorphic to the torus $t_{A_\sigma}/\Omega_{A_\sigma}$ composed with the tangent space at the origin t_{A_σ} and with the period lattice Ω_{A_σ} of A_σ. From the Riemann form associated to L_σ, we get an hermitian norm $\|\cdot\|_{L,\sigma}$ on t_{A_σ} (see for instance [1, § 2.4]). For $\omega\in\Omega_{A_\sigma}$, let A_ω be the smallest abelian subvariety of A_σ such that $\omega\in t_{A_\omega}$. Actually A_ω is an abelian variety defined over a number field K/k of relative degree $\le 2(9g)^{2g}$ (Silverberg [7]). A *period theorem* consists of bounding from above the geometrical degree $\deg_L A_\omega$ in terms of $g,D,\|\omega\|_{L,\sigma}$ and $h_F(A)$. Such a theorem is useful to bound the minimal isogeny degree between two isogeneous abelian varieties ([1, 2, 5, 6]). A *generalized period theorem* consists of replacing ω by a logarithm $u\in t_{A_\sigma}$ of a k-rational point $p\in A(k)$ (we have $\sigma(p)=\exp_{A_\sigma}(u)$). In this setting we have the following bound (written in a very simplified form).

Theorem 3. If $u\neq 0$ then

$$(\deg_L A_u)^{1/(2\dim A_u)}\le\left(D\widehat{h}_L(p)+\|u\|_{L,\sigma}^2\right)\max\left(D+g^g,h_F(A)\right)^{50}.$$

The proof of Theorem 3 extends that of the period theorem [1] using Gel'fond-Baker's method with Philippon-Waldschmidt's approach and some adelic geometry. Since it is long enough, we shall only explain in the rest of the exposition how to deduce Theorem 2 from Theorem 3. The very classical argument is to use the pigeonhole principle. Here we replace it by the more convenient Minkowski's first theorem. Let E be the $\mathbb{R}$-vector space $\mathbb{R}\times t_{A_\sigma}$ endowed with the Euclidean norm

$$\|(a,x)\|^2:=a^2D\widehat{h}_L(p)+\|a.u+x\|_{L,\sigma}^2.$$

In $(E, \|\cdot\|)$ stands the lattice $\mathbb{Z}\times\Omega_{A_\sigma}$ whose determinant is $D\widehat{h}_L(p)\mathrm{h}^0(A,L)^2$. So, by Minkowski, there exists $(\ell,\omega)\in\mathbb{Z}\times\Omega_{A_\sigma}\setminus\{0\}$ such that

$$(\star)\qquad D\widehat{h}_L(\ell p)+\|\ell u+\omega\|^2_{L,\sigma}\leq\gamma_{2g+1}\left(D\widehat{h}_L(p)\mathrm{h}^0(A,L)^2\right)^{1/(2g+1)}$$

where $\gamma_{2g+1}\leq g+1$ is the Hermite constant. Since p is assumed to be non-torsion, the logarithm $\ell u+\omega$ of $\sigma(\ell p)$ is not 0 and Theorem 2 gives a lower bound for the left-hand side of inequality $(\star)$, involving a lower bound for $\widehat{h}_L(p)$. Nevertheless, at this stage, the dimension $\mathrm{h}^0(A,L)$ of the global sections space of the polarization is still in the bound. To remove it, we use Zarhin's trick by replacing A with $(A\times\widehat{A})^4$ (here $\widehat{A}$ is the dual abelian variety), endowed with a principal polarization compatible to L. Then the Néron-Tate height of p remains unchanged whereas Faltings height and dimension of A are multiplied by 8, ruining the numerical constant but also making $\mathrm{h}^0(A,L)$ disappear.

References

[1] É. Gaudron and G. Rémond, *Théorème des périodes et degrés minimaux d'isogénies*, Comment. Math. Helv. **89** (2014), 343–403.

[2] É. Gaudron and G. Rémond, *Polarisations et isogénies*, Duke Math. J. **163** (2014), 2057–2108.

[3] D. Masser, *Small values of heights on families of abelian varieties*, *in* Diophantine approximation and transcendence theory (Bonn, 1985), Lecture Notes in Math. **1290**, (1987), 109–148.

[4] D. Masser, *Letter to Daniel Bertrand*, November 17, 1986.

[5] D. Masser and G. Wüstholz, *Periods and minimal abelian subvarieties*, Ann. of Math. **137** (1993), 407–458.

[6] D. Masser and G. Wüstholz, *Factorization estimates for abelian varieties*, Inst. Hautes Études Sci. Publ. Math. **81** (1995), 5–24.

[7] A. Silverberg, *Fields of definition for homomorphisms of abelian varieties*, J. Pure Appl. Algebra. **77** (1992), 253–262.

[8] B. Winckler, *Intersection arithmétique et problème de Lehmer elliptique*, PhD Thesis (Bordeaux, 2015). 120 pages.

Northcott property for the regulators of number fields and abelian varieties

Fabien Pazuki

1. Introduction

We will divide the talk into four parts. After this introduction, we give in a second part a result concerning families of number fields. In part three, we give a conjectural Northcott property on families of abelian varieties. Finally we focus on the special case of elliptic curves.

Let S be a set. We will say that a function $f: S\to\mathbb{R}$ verifies a Northcott property on S if for any real number B, the set $\{P\in S\,|\,f(P)\leq B\}$ is finite. The goal is to understand to what extent the regulator satisfies such a property in a natural setting.

Studying the regulator in both contexts –number fields and abelian varieties over number fields– is motivated by the following analytic number theory input.

Let K be a number field of degree d, let r_1 be the number of real embeddings, r_2 be the number of pairs of complex embeddings, h_K its class number, R_K its regulator, w_K the number of roots of unity in K and D_K its discriminant. Let ζ_K be the Dedekind zeta function of K. Then the class number formula reads

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}h_K R_K}{w_K\sqrt{|D_K|}}.$$

For abelian varieties over a number field K, the strong form of the conjecture of Birch and Swinnerton-Dyer predicts the value of the first non-zero term in the Taylor expansion of the L-function of A/K at $s = 1$, and the regulator of the Mordell-Weil group $A(K)$ plays an important role in this formula.

2. Number fields

In the case of families of number fields, we prove the following result. Recall that a CM number field is a quadratic imaginary extension of a totally real number field.

Theorem 1. There exists only a finite number of non-CM number fields with bounded regulator.

The main ingredient in the proof is an inequality between the regulator and the discriminant of a number field. We include it here.

Theorem 2. (Silverman [6], Friedman [1]) Let K be a number field of discriminant D_K, regulator R_K and degree d. Let r_K denote the unit rank of K and r_0 the maximum of the unit ranks of proper subfields of K. Then there exists a universal constant $c_1 > 0$ such that

$$R_K \geq c_1 d^{-2d}\left(\log\frac{|D_K|}{d^d}\right)^{r_K - r_0}.$$

It costs some extra efforts to deduce the claimed Northcott property, because the degree d is playing a lot against us in this lower bound. The conclusion is of course obtained by Hermite's theorem, the details are given in [4].

3. Abelian varieties

We now focus on the regulator of abelian varieties over number fields. As in the previous section, the strategy is to lower bound the regulator with a quantity already satisfying a Northcott property. In this context, the Faltings height of A/K seems to be a good choice. To simplify the exposition, we will restrict our study to simple abelian varieties, but the general case is dealt with in [5]. We are able to produce a lower bound on the regulator assuming the following height conjecture.

Conjecture 1. (Lang-Silverman) Let $g \geq 1$ be an integer. For any number field K, there exists a positive constant $c_2 = c_2(K, g)$ such that for any simple abelian variety A/K of dimension g and any ample symmetric line bundle L on A, for any point $P \in A(K)$ that is not in the torsion subgroup, one has

$$\widehat{h}_{A,L}(P) \geq c_2 \max\Big\{h_F(A/K),\, 1\Big\}\,,$$

where $\widehat{h}_{A,L}(.)$ is the Néron-Tate height associated to the line bundle L and $h_F(A/K)$ is the (relative) Faltings height of the abelian variety A/K.

We explain in [5] how to deduce from Minkowski's second theorem the following lower bound.

Proposition 1. Assume Conjecture 1. Let K be a number field, let $g \geq 1$ and $m \geq 0$ be integers. There exist constants $c_3 = c_3(m) > 0$ and $c_4(K, g) > 0$ such that for any simple abelian variety A defined over K of dimension g, of Mordell-Weil rank m, equipped with an ample and symmetric line bundle L,

$$\mathrm{Reg}_L(A/K) \geq c_3(m)\Big(c_4 \max\{h_F(A/K),\, 1\}\Big)^m.$$

It is now easy to obtain the following result.

Theorem 3. Assume Conjecture 1. The set of $\overline{\mathbb{Q}}$-isomorphism classes of simple abelian varieties A, defined over a fixed number field K, of fixed dimension g, with bounded Mordell-Weil rank $m \geq 1$ and bounded regulator is finite.

4. The special case of elliptic curves

By the work of Hindry and Silverman [3], one obtains that Conjecture 1 is true for families of elliptic curves with uniformly bounded Szpiro quotient. As the Szpiro quotient is uniformly bounded by the ABC conjecture (in fact, the ABC conjecture arose while studying this question of bounding the Szpiro quotient), one obtains the following corollary.

Theorem 4. Assume the ABC conjecture. The set of $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves E, defined over a fixed number field K with bounded rank $m_K \geq 1$ and bounded regulator is finite.

References

[1] E. Friedman, *Analytic formulas for the regulator of a number field*. Invent. Math. **98** (1989), 599–622.

[2] M. Hindry and A. Pacheco, *An analogue of the Brauer-Siegel theorem for abelian varieties in positive characteristic*, Moscou Math. J. **16** (2016), 45–93.

[3] M. Hindry and J.H. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. **93** (1988), 419–450.

[4] F. Pazuki, *Heights and regulators of number fields and elliptic curves*, Publ. Math. Besançon **2014/2** (2014), 47–62.

[5] F. Pazuki, *Heights, ranks and regulators of abelian varieties*, arxiv:1506.05165 (2015).

[6] J.H. Silverman, *An inequality relating the regulator and the discriminant of a number field.* Journal of Number Theory **19.3** (1984), 437–442.
[7] J.H. Silverman, *Lower bounds for height functions.* Duke Math. J. **51** (1984), 395–403.

Some Diophantine questions motivated by random walks

Péter P. Varjú
(joint work with E. Breuillard)

1. Problems

I began my talk by posing some questions about the family of polynomials

$$\mathcal{P}_d := \{a_d x^d + \ldots + a_1 x_1 + a_0 : a_0, \ldots, a_d \in \{-1, 0, 1\}\}.$$

The first question is due to Hochman [4].

Question 1. What is the minimum of

$$\{|\xi_1 - \xi_2| \neq 0 : \text{ there are } P_1, P_2 \in \mathcal{P}_d \text{ such that } P_1(\xi_1) = 0 = P_2(\xi_2)\}?$$

The best result I am aware of in this direction is due to Mahler [5], who proved a lower bound of the form $\geq \exp(-Cd \log d)$, where C is an absolute constant. It would be very interesting to know if this bound can be improved. In particular, does the bound $\geq \exp(-Cd)$ hold?

Question 2. Give explicit examples of transcendental numbers ξ such that there is a constant $C > 0$ such that

(a) $|P(\xi)| \geq \exp(-Cd^{100})$, or
(b) $|P(\xi)| \geq \exp(-Cd)$

hold for all $P \in \mathcal{P}_d$.

After my talk, Yann Bugeaud and Evgeniy Zorin provided me with references, where (a) is proved for a large variety of classical constants including values of the exponential function and logarithms and Mahler numbers. In particular, see the references in [3, pp 189]. On the other hand, I am not aware of any results, where (b) is established for an explicit number.

Question 3. Fix a rational number p/q, say in the interval $[9/10, 19/20]$. What is the minimum of

$$\{|P(p/q)| : P \in \mathcal{P}_d\}?$$

We note that the roots of polynomials in $\mathcal{P}_d$ are units, hence $P(p/q)$ is never zero. Since $q^d P(p/q)$ is an integer, we have the trivial lower bound $\geq q^{-d}$ for $P(p/q)$. It would be very interesting to see an improvement on this trivial bound, in particular, a bound of the form $c_{p,q} \exp(-Cd)$ would be very useful in applications. Moreover, even the following weaker form would be sufficient.

Question 4. Is it true that for all rational $p/q \in [9/10, 19/20]$, there is a constant $c_{p,q}$ such that

$$\#\{P \in \mathcal{P}_d : P(p/q) < c_{p,q} \exp(-Cd)\} < \exp(d/100)$$

holds for some absolute constant C?

2. Motivation

The questions posed in the previous section are motivated by recent work on Bernoulli convolutions. Fix a number $\lambda \in (0,1)$ and let $A_0, A_1, \dots$ be a sequence of independent unbiased ± 1-valued random variables. The Bernoulli convolution with parameter λ, denoted by μ_λ, is the distribution of the random variable

$$\sum_{n=0}^{\infty} A_n \lambda^n.$$

It is a long standing open problem to determine the set of parameters such that μ_λ is absolutely continuous. It is easy to see that $\operatorname{supp} \mu_\lambda$ is a Cantor set if $\lambda < 1/2$, hence μ_λ is singular. If the parameter λ is above the critical value of $1/2$ the measure may be absolutely continuous or singular and it is still not fully understood which parameters belong to each class.

We omit an enumeration of new and old results about this problem. Instead we refer the reader to the survey [6] and the more recent papers that we cite below and we focus only on the results that relate to the questions posed in the previous section.

Hochman [4] proved among other results that $\dim \mu_\lambda = 1$ for all $\lambda \in [1/2, 1] \backslash \overline{\mathbf{Q}}$ provided a lower bound $\geq \exp(-Cd)$ holds in Question 1. Unconditionally, he proved that $\dim \mu_\lambda = 1$ holds outside an exceptional set of parameters of dimension 0 and this was furthered by Shmerkin, who proved absolute continuity of μ_λ outside an exceptional set of parameters of dimension 0.

In the upcoming joint paper with Breuillard [2], we prove for any number $\lambda \in (1/2, 1)$ that satisfies (a) in the role of ξ in Question 2 that $\dim \mu_\lambda = 1$. We also prove that Lehmer's conjecture implies $\dim \mu_\lambda = 1$ for all $\lambda \in (a, 1)$ for some $a < 1$. This was previously proved for algebraic values in [1]. Examples satisfying (b) could be used to construct explicit transcendental numbers λ such that μ_λ is absolutely continuous.

Finally, I proved in [7] that there is an absolute constant c such that $\mu_{1-p/q}$ is absolutely continuous for all positive integers p, q satisfying

$$p \leq cq(\log q)^{-1.00001}.$$

The proof relies on the trivial bound q^{-d} for Question 3. A positive answer to Question 4 could be used to prove absolute continuity of μ_λ for all $\lambda \in (a, 1) \cap \mathbf{Q}$ with an absolute constant a.

References

[1] E. Breuillard, P.P. Varjú, *Entropy of Bernoulli convolutions and uniform exponential growth for linear groups*, preprint, arXiv:1510.04043v1, (2015).
[2] E. Breuillard, P.P. Varjú, *Work in progress.*
[3] Y. Bugeaud, *Approximation by algebraic numbers*, Cambridge Tracts in Mathematics, **160** (2004), Cambridge University Press, Cambridge.
[4] M. Hochman, *On self-similar sets with overlaps and inverse theorems for entropy*, Ann. of Math. (2) **180** (2014), no. 2, 773–822.
[5] K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math. J. **11** (1964), 257–262.
[6] Y. Peres, W. Schlag and B. Solomyak, *Sixty years of Bernoulli convolutions*, Fractal geometry and stochastics, II (Greifswald/Koserow, 1998), Progr. Probab., **46**, 39–65.
[7] P.P. Varjú, *Absolute continuity of Bernoulli convolutions for algebraic parameters*, preprint, arXiv:1602.00261v1, (2016).

Around Furstenberg's $\times 2 \times 3$ theorem

Elon Lindenstrauss

In 1967 Furstenberg [2] proved the following theorem:

Theorem 1. Let $x \notin \mathbb{Q}$, and let $a, b \in \mathbb{N}$ be two multiplicatively independent integers. Then $a^n b^k x \bmod 1$ is dense in $[0,1]$.

This theorem highlights a very important phenomenon: rigidity of diagonalizable $\mathbb{Z}^d$-actions when each individual element of the action has no rigidity.

This important theorem raises many questions. For instance, the following question, due also to Furstenberg, is open:

Question 1. Let $1, x, y$ be multiplicatively independent over $\mathbb{Q}$. Is it true that if a, b are relatively prime integers the set

$$\left\{a^n b^k (x,y) \bmod 1 : n,k \in \mathbb{N}\right\}$$

is dense in $[0,1]^2$?

We remark that the following is known (cf. [3] for a closely related result):

Theorem 2 (Wang-L.)**.** Let a, b, c be (pairwise) relatively prime integers. Then the set

$$\left\{a^n b^k c^l (x,y) \bmod 1 : n,k \in \mathbb{N}\right\}$$

is dense in $[0,1]^2$.

However, we do not know if e.g.

$$\left\{a^n b^k c^l (x,y,z) \bmod 1 : n,k,l \in \mathbb{N}\right\}$$

is dense in $[0,1]^3$ if $1, x, y, z$ are linearly independent over $\mathbb{Q}$.

Motivated by a quantitative version of Furstenberg's theorem given by Bourgain, Michel, Venkatesh and the author [1] we present in particular the following question: for $A \subset [0,1]$ let $N(A,\delta)$ denote the minimal number of δ-interval as needed to cover A.

Question 2. Let a, b be multiplicatively independent integers. Are there N, M, K (which may depend on a, b) so that if s, r are integers with $(s, ab) = (s, r) = 1$ then

$$A = \left\{ a^n b^k \frac{r}{s} \bmod 1 : n, k \leq M \log s \right\}$$

satisfy $\log N(A, \log s^{-N}) \geq \frac{1}{K} \log \log s$?

Using Baker's lower bounds for forms in logarithms the answer to the question is affirmative if $|s| < r^{1-\theta}$ for any fixed $\theta > 0$, but we suspect it should be true in the general case.

References

[1] Jean Bourgain, Elon Lindenstrauss, Philippe Michel, and Akshay Venkatesh. Some effective results for $\times a \times b$. *Ergodic Theory Dynam. Systems*, 29(6):1705–1722, 2009.

[2] Harry Furstenberg. Disjointness in ergodic theory, minimal sets, and a problem in Diophantine approximation. *Math. Systems Theory*, 1:1–49, 1967.

[3] Elon Lindenstrauss and Zhiren Wang. Topological self-joinings of Cartan actions by toral automorphisms. *Duke Math. J.*, 161(7):1305–1350, 2012.

Simultaneous rational approximations to manifolds

Victor Beresnevich

(joint work with R. C. Vaughan, S. Velani, E. Zorin)

One of the primary objects for consideration in the metric theory of Diophantine approximation is the set

$$W(n, \psi) = \left\{ \mathbf{y} \in [0,1]^n : |q\mathbf{y} - \mathbf{p}| < \psi(q) \text{ for infinitely many } q \in \mathbb{N},\ \mathbf{p} \in \mathbb{Z}^n \right\},$$

where $\psi : \mathbb{N} \to [0, 1)$ is a function and $n \in \mathbb{N}$ is a fixed dimension. A consequence of several results, essentially due to Khintchine and Jarník, we have the following result

$$\mathcal{H}^s(W(n,\psi)) = \begin{cases} 0 & \text{if} \quad \sum_{q=1}^{\infty} \psi(q)^s q^{n-s} < \infty, \\ \mathcal{H}^s([0,1]^n) & \text{if} \quad \sum_{q=1}^{\infty} \psi(q)^s q^{n-s} = \infty \end{cases}$$

for any monotonic function ψ, where $\mathcal{H}^s$ is the standard s-dimensional Hausdorff measure, $s > 0$.

The content of this report is on the recent progress made in [5] and [6] regarding analogous statements for $W(n, \psi)$ restricted to a submanifold $\mathcal{M}$ of $[0, 1]^n$. The expected statement that comes from a heuristic argument is as follows:

$$\mathcal{H}^s(\mathcal{M} \cap W(n,\psi)) = \begin{cases} 0 & \text{if} \quad \displaystyle\sum_{q=1}^{\infty} \psi(q)^{s+m} q^{-s+d} < \infty\ , \\ \mathcal{H}^s(\mathcal{M}) & \text{if} \quad \displaystyle\sum_{q=1}^{\infty} \psi(q)^{s+m} q^{-s+d} = \infty, \end{cases} \tag{1}$$

where $d = \dim \mathcal{M}$ and $m = \operatorname{codim} \mathcal{M}$ and so $n = d+m$. In all likelihood (1) should hold for arbitrary non-degenerate submanifolds of $\mathbb{R}^n$ as defined in [12], albeit s must be restricted from below. As is well known the problem can be reduced to investigating rational points lying near $\mathcal{M}$ - see [1, 2, 14] or [8]. The corresponding heuristic for counting rational points near $\mathcal{M}$ is as follows:

$$N(\epsilon, Q) \asymp \epsilon^m Q^n, \tag{2}$$

where $N(\epsilon, Q)$ is the number of rational points $\mathbf{p}/q$ ($\mathbf{p} \in \mathbb{Z}^n$, $q \in \mathbb{N}$) with $1 \le q \le Q$ and lying at distance $\le \epsilon$ from $\mathcal{M}$ ($\epsilon < 1$). Again for heuristic (2) to be true for arbitrary non-degenerate manifolds one has to impose a lower bound on ϵ depending on Q (in the case of hypersurfaces one needs $\epsilon \gg Q^{-2}$, see [1]).

In the case of curves in the plane (1) with $s > \frac{1}{2}$ and (2) with $\epsilon > Q^{-2+\delta}$ were proven for arbitrary non-degenerate curves with the best possible condition [2, 7, 9, 14]. In higher dimensions, the divergence case of (1) was proven for arbitrary analytic non-degenerate manifolds [1] under the assumption that $s > \frac{m}{m+1}d$ and in the case of curves, $s > \frac{1}{2}$.

The new results established in [5] given new upper bounds on rational points for a natural subclass of non-degenerate manifolds. Namely, suppose that

$$\mathcal{M}_{\mathbf{f}} := \big\{(\alpha_1, \dots, \alpha_d, f_1(\boldsymbol{\alpha}), \dots, f_m(\boldsymbol{\alpha})) \in \mathbb{R}^n : \boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_d) \in [0,1]^d\big\}$$

where $\mathbf{f} : [0,1]^d \to \mathbb{R}^m$ is C^2 and satisfies the condition that

$$\left| \det \left(\frac{\partial^2 f_j}{\partial \alpha_1 \partial \alpha_i}(\alpha_1, \dots, \alpha_d) \right)_{\substack{1 \le i \le m \\ 1 \le j \le m}} \right| \ge \eta$$

for some fixed positive η. Then (2) is shown to be true, provided

$$\psi(q) \ge q^{-1/(2m+1)} (\log q)^{2/(2m+1)} \qquad \text{for all } q \text{ in the support.}$$

It is worth mentioning that more recently David Simmons [13] has managed to relax the above condition on $\mathbf{f}$ to include a larger subclass of non-degenerate manifolds.

In another direction, [6] deal with the divergence case by generalising the main result of [1] to arbitrary non-degenerate curves in $\mathbb{R}^n$, thus removing the analyticity condition altogether. Both [5] and [6] deal with the inhomogeneous case, which was previously known only in the case of planar curves [4].

References

[1] V. Beresnevich, *Rational points near manifolds and metric Diophantine approximation*, Ann. of Math. (2) **175** (2012), no.1, 187–235.

[2] V. Beresnevich, D. Dickinson, S. Velani, *Diophantine approximation on planar curves and the distribution of rational points*, Ann. of Math. (2) **166** (2007), no.2, 367–426.

[3] V. Beresnevich, F. Ramírez, S. Velani, *Metric Diophantine Approximation: aspects of recent work*, arXiv:1601.01948

[4] V. Beresnevich, R.C. Vaughan, S. Velani, *Inhomogeneous Diophantine approximation on planar curves*, Math. Ann. **349** (2011), no.4, 929–942.

[5] V. Beresnevich, R.C. Vaughan, S. Velani, E. Zorin, *Diophantine approximation on manifolds and the distribution of rational points: contributions to the convergence theory*, To appear in IMRN.
[6] V. Beresnevich, R.C. Vaughan, S. Velani, E. Zorin, *Diophantine approximation on manifolds and the distribution of rational points: contributions to the divergence theory*, Preprint.
[7] V. Beresnevich, E. Zorin, *Explicit bounds for rational points near planar curves and metric Diophantine approximation*, Adv. Math. **225** (2010), no. 6, 3064–3087.
[8] V.I. Bernik, M.M. Dodson, *Metric Diophantine approximation on manifolds*, Cambridge Tracts in Mathematics **137**, Cambridge University Press, Cambridge, 1999.
[9] J.-J., Huang, *Rational points near planar curves and Diophantine approximation*, Adv. Math. **274** (2015), 490–515.
[10] V. Jarník, *Über die simultanen diophantischen Approximationen*, Math. Z. **33** (1931), 505–543.
[11] A. Khintchine, *Zur metrischen Theorie der diophantischen Approximationen*, Math. Z. **24** (1926), 706–714.
[12] D.Y. Kleinbock, G.A. Margulis, *Flows on homogeneous spaces and Diophantine approximation on manifolds*, Ann. of Math. (2) **148** (1998), 339–360.
[13] D. Simmons, *Some manifolds of Khinchin type for convergence*, arXiv:1602.01727.
[14] R.C. Vaughan, S. Velani, *Diophantine approximation on planar curves: the convergence theory*, Invent. Math. **166** (2006), no.1, 103–124.

Diophantine Approximation with quadratic forms

Nikolay Moshchevitin

We study zeros of indefinite rational quadratic forms and related problems in Diophantine approximation.

Let $f(\boldsymbol{x}), \boldsymbol{x} \in \mathbb{R}^n$ be a non-degenerate rational positive defined quadratic form with integer coefficients. Let $F(\boldsymbol{z}) = f(\boldsymbol{x}) - y^2, \boldsymbol{z} = (\boldsymbol{x}, y) \in \mathbb{R}^{n+1}$ be the corresponding indefinite form. We suppose $F(\boldsymbol{z})$ to be isotropic over $\mathbb{Q}$.

We discuss three diffrent approaches related to the study of small zeros of F.

1. In 1937 Venkov [16] introduced a multidimensional generalization of continued fractions' algorithm related to the analysis of the convex hull of all integer points inside the cone $F(\boldsymbol{z}) > 0$. This construction was motivated by earlier works by Voronoi [18]. By means of geometric argument, he proved that the fundamental domain of the action of the group of integer automorphisms of $F(\boldsymbol{z})$ is bounded and is determined by a finite number of facets of the convex hull under consideration. In [17] he generalized some of his earlier results.

In fact, this result by Venkov leads to a certain upper bound for the smallest zero of $F(\boldsymbol{z})$. However Venkov did not deduced such a corollary of his theorems by himself.

2. In 1955 Cassels [2] proved an elegant theorem about existence of small zeroes of isotropic quadratic forms.

Theorem 1. (Cassels). Consider a quadratic form

$$Q(\boldsymbol{\xi}) = \sum_{i,j=1}^{d} Q_{i,j}\xi_i\xi_j, \;\; Q_{i,j} = Q_{j,i}$$

and define $Q = \max|Q_{i,j}|$. If Q is isotropic then there exists $\mathbf{g} = (g_1, ..., g_d) \in \mathbb{Z}^d \setminus \{\mathbf{0}\}$ with $Q(\mathbf{g}) = 0$ and

$$\max|g_k| \leq (3Q)^{\frac{d-1}{2}}.$$

This theorem was generalized and extended by many authors (see [1, 4, 12, 13, 14, 15]). An excellent introductory exposition (which includes simple theorems on intrinsic approximation, both in real and p-adic cases) one can find in Cassels' book [3]. A survey on some further results is due to Fukshansky [5].

In particular, it is known [3] that the upper bound $\ll Q^{\frac{d-1}{2}}$ is optimal. Additional information about the signature of Q (or the maximal dimension of subspace over which Q varnishes) gives an improvement of this upper bound [12]. The optimality of these and more general bounds is well known also [13, 14]. Also it is known that under the conditions of Cassels' theorem one can find a collection of d *linearly independent* zeros of Q (see [15]).

3. Quite recently Fishman, Kleinbock, Merrill and Simmons [9, 5] proved a series of dynamical results related to intrinsic approximations on spheres and quaratic surfaces. In the first paper Kleinbock and Merrill [9] consider the simplest quadratic form $f(\boldsymbol{x}) = x_1^2 + ... + x_n^2$. In our notation, one of the general results from the second paper [5] may be formulated as follows.

Theorem 2. There exists $\kappa_f > 0$ with the following property. Let $f(\boldsymbol{\alpha}) = f(\alpha_1, ..., \alpha_n) = 1$. Let $\boldsymbol{\alpha} \notin \mathbb{Q}^n$. If F is isotropic, then there exist infinitely many vectors

$$\mathbf{r} = \left(\frac{a_1}{q}, ..., \frac{a_n}{q}\right), \quad a_1, ..., a_n \in \mathbb{Z}, \quad q \in \mathbb{Z},$$

with

$$f(\mathbf{r}) = f\left(\frac{a_1}{q}, ..., \frac{a_n}{q}\right) = 1$$

and

$$\sqrt{f(\boldsymbol{\alpha} - \mathbf{r})} \leq \frac{\kappa_f}{q}.$$

This result has a "uniform" (Dirichlet-type) version. The set of $\boldsymbol{\alpha}$ for which the result is sharp in order is of full Hausdorff dimension.

We join all these settings together and give some new elementary results related to the geometry of numbers only. Some of our results are presented in [10, 11].

In particular we give a very easy proof of an effective version of a result of Theorem 2 concerning intrinsic approximation. Our proof relies on Cassels' Theorem 1 and Minkowski's theorem on successive minima. We give an effective bound for κ_f (see [11]). In the case $n = 2, f(\boldsymbol{x}) = x_1^2 + x_2^2$ we calculate the optimal value for the constant κ_f [10]. This improves on earlier results by Hlawka [8] and Fukshansky [6]. In the case $n = 3, f(\boldsymbol{x}) = x_1^2 + x_2^2 + x_3^2$ we give a proof which relies on Minkowski's convex body theorem only, and calculate the value of the constant κ_f which is close to the optimal one [10].

Our research is supported by RNF grant 14-11-00433.

References

[1] B. J. Birch, H. Davenport, *Quadratic equations in several variables*, Mathematical Proceedings of the Cambridge Philosophical Society, **54**:2 (1958), 135–138.
[2] J. W. S. Cassels, *Bounds for the least solutions of homogeneous quadratic equations*, Mathematical Proceedings of the Cambridge Philosophical Society, **51**:2 (1955), 262–264.
[3] J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press, 1978.
[4] H. Davenport, *Note on a theorem of Cassels*, Mathematical Proceedings of the Cambridge Philosophical Society, **53**:2 (1957), 539–540.
[5] L. Fishman, D. Kleinbock, K. Merrill, D. Simmons, *Intrinsic Diophantine approximation on manifolds*, preprint available at arXiv:1405.7650v4[math.NT] 24 Sep 2015.
[6] L. Fukshansky, *On similarity classes of well-rounded sublattices of* $\mathbb{Z}^2$, Journal of Number Theory 129 (2009), 2530–2556.
[7] L. Fukshansky, *Heights and quadratic forms: Cassels' theorem and its generalizations*, Contemp. Math., **587** (2013), 77–94.
[8] E. Hlawka, *Approximation von Irrationalzahlen und pythagoräische Tripel*, Bonner Mathemati-sche Schriften, 121 (1980), 1–32.
[9] D. Kleinbock, K. Merrill, *Rational approximation on Spheres*, Isr. J. Math. **209** (2015), Part 1, 293–322.
[10] N. Moshchevitin, *Über die rationalen Punkte auf der Sphäre*, Monatsh. Math. **179**: 1 (2016), 105–112.
[11] N. Moshchevitin, *Eine Bemerkung ber positiv definite quadratische Formen und rationale Punkte*, preprint available at arXiv:1510.06214v3.
[12] H.P. Schlickewei, *Kleine Nullstellen homogener quadratischer Gleichungen* , Monatshefte für Mathematik, **100** (1985), 35–45.
[13] H.P. Schlickewei, W.M. Schmidt, *Quadratic Forms Which Have Only Large Zeros I*, Monatshefte für Mathematik, **105** (1988), 295–311.
[14] H.P. Schlickewei, W.M. Schmidt, *Isotrope Unterräume rationaler quadratischer Formen*, Mathematische Zeitschrift, **201** (1989), 191–208.
[15] R. Schulze-Pillot, *Small linearly independent zeros of quadratic forms*, Monatshefte für Mathematik, **95** (1983), 24–249.
[16] B.A. Venkov *On the arithmetic group of automorphisms of indefinite quadratic form*, Izvestiya AN SSSR, ser. Matematicheskaya **1**: 2 (1937), 139–170 (in Russian).
[17] B.A. Venkov *On indefinite quadratic forms with integer coefficients*, Trudy MIAN SSSR (Proceedings of Steklov Mathematical Institute of Russian Academy of Sciences), v. 38 (1951), 30–41 (in Rusian).
[18] G. Voronoi, *Sur quelques propriétés des formes quadratiques positives parfaites*, Crelle Journal, **133** (1908) 97–178.

Kummer theory on abelian varieties over function fields

Daniel Bertrand

1. Division points and logarithms

Let K be a number field, and let A be an abelian variety over K. The following Kummer theorical result, which is essentially due to K. Ribet [20], has been applied to transcendence problems (see [4]), to the Manin-Mumford conjecture (see [11]), and to various questions of linear dependence, see [9], [14], [15], [3], [18], [12].

Theorem 1. Let y be a point of $A(K)$, and let B be the smallest abelian subvariety of A such that a multiple of y by a non-zero integer lies in $B(K)$. There exists a

positive constant $c = c(A, K, y)$ such that for any positive integer n, any n-division point $\frac{1}{n}y$ of y in $A(K^{\mathrm{alg}})$ generates a field of degree $\geq cn^{2\dim(B)}$ over K.

The aim of the present work is the following analogue of Theorem 1, where K is replaced by the function field $\mathbb{K} = \mathbb{C}(S)$ of an algebraic curve $S/\mathbb{C}$ (see [5], §5). So, A is now an abelian variety over $\mathbb{K}$, and we denote its $\mathbb{K}/\mathbb{C}$-trace by A_0. We then have :

Theorem 2. Let y be a point of $A(\mathbb{K})$, and let B be the smallest abelian subvariety of A such that a multiple of y by a non-zero integer lies in $B(\mathbb{K}) + A_0(\mathbb{C})$. There exists a positive constant $c = c(A, \mathbb{K}, y)$ such that for any positive integer n, any n-division point $\frac{1}{n}y$ of y in $A(\mathbb{K}^{\mathrm{alg}})$ generates a field of degree $\geq cn^{2\dim(B)}$ over $\mathbb{K}$.

Ribet's proof (the Bashmakov method, see [16]) can be tracked back to [22], and is based on a collection of "axioms", known to hold by work of Faltings and Serre [21]. One of these axioms is the Tate conjecture on Galois invariant endomorphisms, whose functional analogue *does not* always hold (even when $A_0 = 0$, see [8], [10], [23]). In order to remedy this problem, we appeal to Y. André's logarithmic version of the Ax-Schanuel problem for A ([1], see also [5], [2]), which asserts that keeping the notation of Theorem 2 and writing $\tilde{y} \in \tilde{A}(\mathbb{K})$ for any lift of $y \in A(\mathbb{K})$ to the universal extension $\tilde{A}$ of A.

Theorem 3. Any logarithm $\tilde{x}$ of $\tilde{y}$ in $\mathrm{Lie}(\tilde{A})$ generates a field of transcendence degree $2\dim(B)$ over $\mathbb{K}$.

The deduction of Theorem 2 from Theorem 3 is based on Nori's theorem on strong approximation in (non necessarily semi-simple) linear algebraic groups, see [19], Theorem 5.4, and below.

2. Main issues

The three statements reflect large sizes of Galois groups (relative to well-chosen intermediate fields), as well as independence of ℓ-adic representations, in the sense of Serre (see [7], [6]).

For instance, one of the steps towards Theorem 1 reads as follows. The intermediate field is $K_\infty = K(A_{\mathrm{tor}})$, with (profinite) Galois group $J := \mathrm{Gal}(K_\infty/K)$. Then for any large enough prime number ℓ, the image of $N_y := \mathrm{Gal}(K_\infty(\frac{1}{\ell}y)/K_\infty)$ under its natural embedding in $A[\ell]$ fills up $B[\ell]$. The proof is the same as Ribet's. The required vanishing of $H^1(J, A[\ell])$ follows from the construction of a suitable central element of J, itself deduced from Serre's theorem on homotheties.

For Theorem 3, the intermediate field is the Picard-Vessiot extension $\mathbb{K}^\sharp = \mathbb{K}((L\tilde{A})^\nabla)$ of $\mathbb{K}$ attached to the Gauss-Manin connection ∇ on the Lie algebra $L\tilde{A}$, with $(L\tilde{A})^\nabla \simeq T(A) \otimes \mathbb{C}$, where $T(A) = H_1(A_s, \mathbb{Z})$ for some fiber A_s of the corresponding abelian scheme over S. Then, the image of the differential Galois group $\mathbb{N}_y := Gal(\mathbb{K}^\sharp(\tilde{x})/\mathbb{K}^\sharp)$ under its natural embedding in $T(A) \otimes \mathbb{C}$ fills up

$T(B) \otimes \mathbb{C}$. The proof is based on the semi-simplicity of $\mathbb{J} = \mathrm{Gal}(\mathbb{K}^\sharp/\mathbb{K})$, and on Manin's theorem of the kernel.

Finally, let Γ_y be the image of the topological fundamental group $\pi_1(S, s)$ in its action on the $\mathbb{Z}$-local system $\mathcal{P}_y$ formed by all logarithms of all multiples of $\tilde{y}$. Since ∇ is Fuchsian, $\mathbb{G}_y = \mathrm{Gal}(\mathbb{K}^\sharp(\tilde{x})/\mathbb{K})$ is the Zariski closure of Γ_y in $\mathrm{Aut}(\mathcal{P}_{y,s} \otimes \mathbb{C})$. Let G_y be the group scheme over $\mathbb{Z}$ defined by $\mathbb{G}_y$ and the lattice $\mathcal{P}_{y,s}$. Similarly, let $N_y = T(B)$ be the corresponding $\mathbb{Z}$-form of the unipotent radical $\mathbb{N}_y$ of $\mathbb{G}_y$. Notice that $\Gamma_y \subset G_y(\mathbb{Z})$ will usually intersect $N_y(\mathbb{Z})$ only at the origin.

We now recall Nori's theorem, over a general ring $R = \mathbb{Z}[\frac{1}{d}]$, with $\hat{R} = \Pi_{(\ell,d)=1}\mathbb{Z}_\ell$.

Theorem 4. (see [19]). Let G be a subgroup scheme of $\mathrm{GL}_{m/R}$, and let Γ be a finitely generated subgroup of $G(R)$, Zariski dense in G. Assume that $G(\mathbb{C})$ is connected and simply connected. Then, the closure $\overline{\Gamma}$ of Γ in $G(\hat{R})$ is open in $G(\hat{R})$.

Since $\mathbb{J}$ is semi-simple, we can apply this to the universal cover $\tilde{G}_y$ of G_y (see [13], p. 347, for this type of reduction). The isogeny $\tilde{G}_y \to G_y$ induces an isomorphism on the unipotent radical N_y, and we deduce that $\overline{\Gamma_y} \cap N_y(\hat{\mathbb{Z}})$ is open in $N_y(\hat{\mathbb{Z}})$. In particular, its image under reduction mod ℓ, resp. ℓ^n, coincides with $N_y(\mathbb{F}_\ell) \simeq B[\ell]$ for almost all ℓ, resp. has bounded index in $B[\ell^n]$ for each ℓ. This concludes the proof of Theorem 2.

3. Effectivity

We here restrict to Theorem 1. The dependence of $c(A, K, y)$ in terms of A and K relies on effective versions of Ribet's axioms, which can partly be achieved thanks to the theorems of Masser-Wüstholz on minimal periods and their sharpening by Gaudron-Rémond. But a control on the vanishing of $H^1(J, A[\ell^n])$ seems out of reach in general (see however [17], 8.3.12, for a related property of Teichmüller lifts).

As for the dependence of $c(A, K, y)$ in the point y, one may wonder if it could just disappear under the natural assumption that y be a *primitive* point of $A(K)$, meaning that for any $\beta \in \mathcal{O} := \mathrm{End}(A)$, y lies in $\beta(A(K))$ only if $\beta \in \mathcal{O}^*$. Here is a counterexample.

Let $A = E$ be a CM elliptic curve over K, of $\mathcal{O}$-rank 1, with $h(\mathcal{O}) = 2$. Assume that the $\mathcal{O}$-module $E(K)$ has no torsion, but is not free, say $E(K) \simeq \mathfrak{p}$ for a non-principal prime ideal. For any prime $\ell = \mathfrak{l}\bar{\mathfrak{l}}$ split into non-principal ideals, $\mathfrak{p}\mathfrak{l} = \mathcal{O}.y_\ell$ is principal, and its generator y_ℓ is a primitive point of $E(K)$. Indeed, if $y_\ell = \beta z$ for some $\beta \in \mathcal{O}, z \in \mathfrak{p}$, then $N(y_\ell) = p\ell, N(z) = pn$ with $n > 1$ (otherwise, z would generate $\mathfrak{p}$), so $N(\beta)n = \ell$ and $N(\beta) = 1$.

For any $\alpha \in \bar{\mathfrak{l}} \setminus \mathfrak{l}$ (hence not divisible by ℓ in $\mathcal{O}$), $\alpha.y_\ell \in \bar{\mathfrak{l}}\mathfrak{p}\mathfrak{l} = \ell E(K)$, i.e. there is a point $z_\ell \in E(K)$ such that $\alpha.y_\ell = \ell z_\ell$. Setting $K_\ell = K(E[\ell])$, we get $\mathrm{Gal}(K_\ell(\frac{1}{\ell}y_\ell)/K_\ell) \simeq E[\bar{\mathfrak{l}}]$, of order ℓ only. In fact, there is a constant $c' = c'(\mathcal{O})$ and

an $\alpha \in \bar{\mathfrak{l}} \setminus \mathfrak{l}$ such that $\frac{1}{\ell} y_\ell = \frac{1}{\alpha} z_\ell$ generates over K a field of degree $\leq c'\ell = o(\ell^2)$. This shows that $c(E, K, y_\ell)$ must depend on the primitive point y_ℓ.

References

[1] Y. André : Mumford-Tate groups of mixed Hodge structures and the theorem of the fixed part; Compositio Math., 82 (1992), 1–24.

[2] J. Ayoub : Periods and the conjectures of Grothendieck and Kontsevich-Zagier; EMS Newsletter 91 (2014), 12–18.

[3] G. Banaszak, W. Gajda, P. Krason : Detecting linear dependence by reduction maps; J. Number Theory 115 (2005), 322–342.

[4] D. Bertrand : Galois representations and transcendental numbers; in *New Advances in Transcendence Theory*, ed. A. Baker, pp. 37–55, Cambridge UP 1988.

[5] D. Bertrand, Galois descent in Galois theories; Sém. et Congrès 23 (2011), Societé Math. France, 1–24.

[6] G. Böckle, W. Gajda, S. Petersen : Independence of ℓ-adic representations of geometric Galois groups; J. reine angew. Math., to appear.

[7] A. Cadoret : An open adelic image theorem for abelian schemes; IMRN, to appear.

[8] P. Deligne : Théorie de Hodge II; Publ. Math. IHES, 40 (1971), 15–58.

[9] R. Dvornicich, U. Zannier : Local-global divisibilty in some commutative algebraic groups; Bull. Soc. math. France 129 (2001), 317–338.

[10] G. Faltings : Arakelov's Theorem for Abelian Varieties; Invent. math. 73 (1983), 337–347.

[11] M. Hindry : Autour d'une conjecture de Serge Lang; Invent. math. 94 (1988), 575–603.

[12] P. Jossen : Detecting linear dependence on an abelian variety via reduction maps; Comment. Math. Helv. 88 (2013), 323–352.

[13] N. Katz : Report on the irreduciblity of L-functions; in *Number Theory, Analysis and Geometry* (in mem. S. Lang), eds D. Goldfeld et al., Springer, 2012, 321–353.

[14] C. Khare, D. Prasad : Reduction of homomorphisms mod p and algebraicity; Journal of Number Theory 105 (2004), 322–332.

[15] E. Kowalski : Some local-global applications of Kummer theory; Manuscripta math. 111 (2003), 105–139.

[16] S. Lang : *Elliptic curves : Diophantine analysis*; Springer GMW 231, 1978.

[17] D. Lombardo : Représentations galoisiennes et groupe de Mumford-Tate associé à une variété abélienne; Thèse Univ. Paris Sud, Déc. 2015.

[18] T. Matev : Good reduction of 1-motives; PhD thesis, Univ. Bayreuth, 2013.

[19] M. Nori : On subgroups of $GL_n(\mathbb{F}_p)$; Invent. math. 88 (1987), 257–275.

[20] K. Ribet : Kummer theory on extensions of abelian varieties by tori; Duke Math. J. 46 (1979), 745–761.

[21] J-P. Serre : Résumé du cours de 1985-86; in *Oeuvres IV*, 136, 33–37, Springer, 2000.

[22] J. Tate : letter to J-P. Serre, Jan 14, 1970, in *Correspondance Serre-Tate*, Doc. math. 13 (2015), Soc. Math. France, p. 389.

[23] Yu. Zarhin : Isogeny classes of abelian varieties over function fields; Proc. London Math. Soc. 96 (2008), 312–334.

Torsion subvarieties and Betti maps

Pietro Corvaja
(joint work with Y. André, D. Masser, U. Zannier)

Let $\mathcal{C}$ be a (complex) algebraic curve and $\mathcal{A} \to \mathcal{C}$ be a family of abelian varieties, i.e. a morphism of algebraic varieties whose generic fiber is an abelian variety. Given a section $s : \mathcal{C} \to \mathcal{A}$ we say that a point $p \in \mathcal{C}$ is torsion if $s(p)$ is a torsion point on the abelian variety $\mathcal{A}_p$ lying over p.

A particular case of a celebrated conjecture by Pink (see [2], page 78) reads as follows.

Conjecture 1. If the relative dimension of $\mathcal{A}$ over $\mathcal{C}$ is at least two and $s(\mathcal{C})$ is not contained in a proper algebraic sub-group scheme, then there exist only finitely many torsion points for s.

On the contrary, it is not difficult to prove that if $\mathcal{A} \to \mathcal{C}$ is a non-constant family of elliptic curves, then every section admits infinitely many torsion points.

The above Conjecture was proved by Masser and Zannier in the case the abelian scheme is isogenous to a product of elliptic schemes [3] and, even for simple abelian schemes, when the ground field is the field of algebraic numbers [4].

A first goal of this research was proving the general case, for a simple abelian scheme (over a curve defined over the complex number field). In solving this problem, we had to treat abelian schemes over arbitrary bases.

Given an algebraic variety S of arbitrary dimension and an algebraic family of abelian varieties $\mathcal{A} \to S$ provided with a section $s : S \to \mathcal{A}$, we call *torsion subvariety* any (closed) algebraic subvariety $Y \subset S$ where the restriction of s is a torsion section. Our general result is as follows.

Theorem 1 (P. Corvaja, D. Masser, U.Zannier)**.** Let S be a complex algebraic variety, $\mathcal{A} \to S$ an abelian scheme over S and $s : S \to \mathcal{A}$ be a section. If the relative dimension of $\mathcal{A}$ over S is two and $s(S)$ is not contained in any algebraic sub-group scheme, then there exist only finitely many torsion hypersurfaces.

A main tool in the proof is represented by the so called *Betti map*, i.e. the 'logarithm' of the section. More precisely, locally (on S) one can: (1) trivialize the tangent spaces to $\mathcal{A}_p$ at the origin, by identifying them with $\mathbb{C}^g$ (where g is the dimension of the abelian variety $\mathcal{A}_p$); (2) define a logarithm of the section s as a holomorphic map to $\mathbb{C}^g$; (3) define a basis of the periods for the abelian exponential map, as $2g$ holomorphic maps to $\mathbb{C}^g$; and finally express the logarithm as a linear combination of this basis of periods,with real coefficients. One then obtains a locally well defined map $S \to \mathbb{R}^{2g}$, which is called the Betti map.

A celebrated theorem of Yu. Manin [1] states that such a map cannot be constant if the section is non-torsion and the family admits no 'fixed part'.

We provide some results on the rank of the differential of this map; for instance, we prove the following statement.

Theorem 2 (Y. André, P. Corvaja, U. Zannier)**.** Let $\mathcal{A} \to S$ be an algebraic family of principally polarized abelian varieties of dimension g and let $s \to \mathcal{A}$ be a section, not contained in any algebraic sub-group scheme. Let d be the dimension of the image of S in the moduli space of principally polarized abelian varieties of dimension g. Then, if $\min(d, g) \leq 2$, the differential of the Betti map has generic rank $2\min(d, g)$.

This research, still in progress, has been done in collaboration with Y. André, D. Masser and U. Zannier, inside the research project *Arithmetic Algebraic Geometry and Number Theory*, PRIN 20105LL47Y-001.

References

[1] Yu. Manin, Rational points on curves over function fields, Izv. Akad. Nauk SSSR Ser. Mat, **7** (1963), 1395–14140.
[2] U. Zannier, *Some Problems of Unlikely Intersections in Arithmetic and Geometry*, Annals of Mathematics Studies **181**, Princeton University Press, Princeton, NJ (2012).
[3] D. Masser, U. Zannier,*Torsion points on families of squares of elliptic curves* , Math. Annalen **352** (2012), 453–484.
[4] D. Masser, U. Zannier, *Torsion points on families of simple abelian surfaces and Pell's equation over polynomial rings*, Journal European Math. Soc. **17** (2015), 2379–2416.

Bi-algebraic system on the universal vectorial extension

Ziyang Gao

1. Universal vectorial extension

1.1. **Universal vector extension of an abelian variety.** Let A be an abelian variety over $\mathbb{C}$. By a *vector extension* of A, we mean an algebraic group E such that there exist a vector group W and an exact sequence $0 \to W \to E \to A \to 0$. There exists a universal vector extension $A^\natural$ of A such that any vector extension of A is obtained as $E \cong A^\natural \times^{W_A} W$:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W_A & \longrightarrow & A^\natural & \longrightarrow & A & \longrightarrow & 0 \\ & & \vdots & & \downarrow & & \downarrow{=} & & \\ 0 & \longrightarrow & W & \longrightarrow & E & \longrightarrow & A & \longrightarrow & 0 \end{array}$$

In fact $A^\natural$ is constructed as follows. Consider the Hodge decomposition $H^1(A, \mathbb{C}) = H^{0,1}(A) \oplus H^{1,0}(A)$. The holomorphic part $H^{1,0}(A)$ is dual to the tangent space t_A of A at 0, and $A \cong t_A/H_1(A, \mathbb{Z})$. The anti-holomorphic part $H^{0,1}(A)$ is dual to $\omega_{A^\vee}$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^{0,1}(A)^\vee & \longrightarrow & H^1(A, \mathbb{C})^\vee & \longrightarrow & H^{1,0}(A)^\vee = t_A & \longrightarrow & 0 \\ & & \downarrow{=} & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \omega_{A^\vee} & \longrightarrow & A^\natural & \longrightarrow & A & \longrightarrow & 0 \end{array}$$

In particular, we have the uniformization $H^1(A,\mathbb{C})^\vee \cong \mathbb{C}^{2g} \to A^\natural$.

1.2. **Universal vectorial extension.** Let A_g be a fine moduli space of principally polarized abelian varieties and let $\mathfrak{A}_g$ be the universal family over A_g. By a *vector extension* of $\mathfrak{A}_g$, we mean a group scheme E over A_g such that there exist a vector group W over A_g and an exact sequence $0 \to W \to E \to \mathfrak{A}_g \to 0$ of group schemes over A_g. The universal vector extension $\mathfrak{A}_g^\natural$ of $\mathfrak{A}_g$ exists and we call it the *universal vectorial extension*. It satisfies $0 \to \omega_{\mathfrak{A}_g^\vee/A_g} \to \mathfrak{A}_g^\natural \to \mathfrak{A}_g \to 0$ and any vector extension E of $\mathfrak{A}_g$ is a push-out $E = \mathfrak{A}_g^\natural \times^{\omega_{\mathfrak{A}_g^\vee/A_g}} W$.

The construction of $\mathfrak{A}_g^\natural$ is similar as before: the dual of the first relative de Rham cohomology $\mathcal{H}^1_{dR}(\mathfrak{A}_g/A_g)^\vee$ is a variation of Hodge structures of type $\{(-1,0),(0,-1)\}$. Let $\mathcal{F}^0\mathcal{H}^1_{dR}(\mathfrak{A}_g/A_g)^\vee \subset \mathcal{H}^1_{dR}(\mathfrak{A}_g/A_g)^\vee$ be the Hodge filtration. Then $\mathcal{F}^0\mathcal{H}^1_{dR}(\mathfrak{A}_g/A_g)^\vee \cong \omega_{\mathfrak{A}_g^\vee/A_g}$ and we have

(1)

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{F}^0\mathcal{H}^1_{dR}(\mathfrak{A}_g/A_g)^\vee & \longrightarrow & \mathcal{H}^1_{dR}(\mathfrak{A}_g/A_g)^\vee & \longrightarrow & \frac{\mathcal{H}^1_{dR}(\mathfrak{A}_g/A_g)^\vee}{\mathcal{F}^0\mathcal{H}^1_{dR}(\mathfrak{A}_g/A_g)^\vee} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle =} & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \omega_{\mathfrak{A}_g^\vee/A_g} & \longrightarrow & \mathfrak{A}_g^\natural & \longrightarrow & \mathfrak{A}_g & \longrightarrow & 0
\end{array}$$

1.3. **Uniformization.** The uniformization of $\mathfrak{A}_g^\natural$ is $\mathbb{C}^{2g} \times \mathcal{H}_g^+$, where $\mathcal{H}_g^+$ is the Siegel upper half plane. Let $\mathcal{V} := \mathbb{C}^{2g} \times \mathcal{H}_g^+$. Each point $x \in \mathcal{H}_g^+$ gives a $\mathbb{Q}$-Hodge structure of type $\{(-1,0),(0,-1)\}$, so $\mathcal{V}$ is a variation of Hodge structures over $\mathcal{H}_g^+$ and we have a Hodge filtration $\mathcal{F}^0\mathcal{V} \subset \mathcal{V}$. The group $\mathrm{GSp}_{2g}(\mathbb{R})^+$ acts on $\mathcal{V}$ by $g(v,x) = (gv, gx)$. Suppose $A_g \cong \Gamma\backslash\mathcal{H}_g^+$, where $\Gamma \subset \mathrm{Sp}_{2g}(\mathbb{Z})$ is a neat subgroup. Then $\Gamma\backslash\mathcal{F}^0\mathcal{V} \cong \omega_{\mathfrak{A}_g^\vee/A_g}$.

The holomorphic bundle $\mathcal{V}/\mathcal{F}^0\mathcal{V}$ over $\mathcal{H}_g^+$ can be viewed as follows. As a smooth bundle it is $\mathbb{R}^{2g} \times \mathcal{H}_g^+$, and the complex structure of the fiber over $x \in \mathcal{H}_g^+$ is the identification $\mathbb{R}^{2g} \cong \mathbb{C}^g$, $(a,b) \mapsto a + xb$ (when $g = 1$, this is $(a,b) \mapsto a + \tau b$ for any $\tau \in \mathcal{H}^+$). Hence $(\mathbb{Z}^{2g} \rtimes \Gamma)\backslash(\mathcal{V}/\mathcal{F}^0\mathcal{V}) \cong \mathfrak{A}_g$.

1.4. **The Deligne-Pink language.** To sum it up, let us define the following pair $(P_{2g}, \mathcal{X}_{2g}^\natural)$:

- P_{2g} is the $\mathbb{Q}$-group $V_{2g} \rtimes \mathrm{GSp}_{2g}$, where V_{2g} is the $\mathbb{Q}$-vector group of dimension $2g$ and GSp_{2g} acts on V_{2g} by the natural representation;
- $\mathcal{X}_{2g}^\natural$ is $\mathbb{C}^{2g} \times \mathbb{H}_g^+$ as sets, with the action of $P_{2g}(\mathbb{R})^+V_{2g}(\mathbb{C})$ on $\mathcal{X}_{2g}^\natural$ defined by $(v,g)\cdot(v',x) := (v + gv', gx)$ for $(v,g) \in P_{2g}(\mathbb{R})^+V_{2g}(\mathbb{C})$ and $(v',x) \in \mathcal{X}_{2g}^\natural$. This action is transitive.

Let Γ be a neat subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z})$. We have (see [5])

Theorem 1 (Gao)**.** The quotient $\mathfrak{A}_g^\natural := (\mathbb{Z}^{2g} \rtimes \Gamma)\backslash(\mathbb{C}^{2g} \times \mathcal{H}_g^+)$ is the universal vector extension of the universal abelian variety over the fine moduli space $A_g := \Gamma\backslash\mathcal{H}_g^+$.

2. Bi-algebraic system on $\mathfrak{A}_g^\natural$

2.1. **Arithmetic bi-algebraic system.** We study the uniformization denoted $\mathrm{unif}\colon \mathbb{C}^{2g}\times\mathcal{H}_g^+\to\mathfrak{A}_g^\natural$. The algebraic variety $\mathfrak{A}_g^\natural$ is defined over $\bar{\mathbb{Q}}$. Denote by $\pi^\natural\colon \mathfrak{A}_g^\natural\to A_g$. The arithmetic bi-algebraic property of unif is summarized in the following theorem, which follows from two theorems of Wüstholz [8] and Cohen, Shiga-Wolfart [6]. See Ullmo [7].

Theorem 2. For any point $u\in\bar{\mathbb{Q}}^{2g}\times\mathcal{H}_g^+(\bar{\mathbb{Q}})$, the following statements are equivalent.

(1) $\mathrm{unif}(u)\in\mathfrak{A}_g^\natural(\bar{\mathbb{Q}})$;
(2) $\pi^\natural(\mathrm{unif}(u))$ is a CM point of A_g and u is a torsion point on its fiber of $\pi^\natural$.

2.2. **Geometric bi-algebraic system.** We endow $\mathbb{C}^{2g}\times\mathcal{H}_g^+$ with the following complex algebraic structure: $\mathcal{H}_g^+$ is an open subset of $\mathbb{C}^{g(g+1)/2}$ and we say that a subset Z of $\mathbb{C}^{2g}\times\mathcal{H}_g^+$ is *algebraic* if it is the intersection of its Zariski closure in $\mathbb{C}^{2g+g(g+1)/2}$ with $\mathbb{C}^{2g}\times\mathcal{H}_g^+$. We say that an irreducible subvariety $Y^\natural$ of $\mathfrak{A}_g^\natural$ is *bi-algebraic* if one (and hence all) complex analytic irreducible component of $\mathrm{unif}^{-1}(Y)$ is algebraic. We hope to characterize all the bi-algebraic subvarieties of $\mathfrak{A}_g^\natural$.

Let $Y^\natural$ be a subvariety of $\mathfrak{A}_g^\natural$. Use the following notation:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \omega_{\mathfrak{A}_g^\vee/A_g} & \longrightarrow & \mathfrak{A}_g^\natural & \xrightarrow{p} & \mathfrak{A}_g & \longrightarrow & 0, \\ & & & & \downarrow{\scriptstyle \pi^\natural} & \swarrow{\scriptstyle \pi} & & & \\ & & & & A_g & & & & \end{array} \qquad \begin{array}{ccc} Y^\natural & \longmapsto & Y. \\ \downarrow & & \\ B & & \end{array}$$

Then $\mathfrak{A}_g|_B:=\pi^{-1}(B)$ is an abelian scheme over B. Let $\mathcal{C}$ be its isotrivial part.

Theorem 3 (Gao)**.** ([3, Corollary 8.3], [4, Proposition 3.3]) Y is bi-algebraic iff

(1) B is a totally geodesic subvariey of A_g;
(2) Y is the translate of an abelian subscheme by a torsion section and then by a constant section of $\mathcal{C}\to B$.

First of all, note that if Y is a point, then $Y^\natural$ is always bi-algebraic and it can be any subvariety of $\mathbb{C}^{2g}$. So the characterization of bi-algebraic subvarieties of $\mathfrak{A}_g^\natural$ cannot be as neat as for $\mathfrak{A}_g$. However we show that this is the only problem.

Assume that Y/B is an abelian scheme (e.g. if Y is bi-algebraic), then $\mathfrak{A}_g^\natural|_Y:=p^{-1}(Y)$ is a vector extension of Y which contains $Y^\natural$ as a subvariety. In fact we have a decomposition

$$\mathfrak{A}_g^\natural|_Y = Y^{univ}\times_B\left(\omega_{\pi^{-1}(B)^\vee/B}\big/\omega_{Y^\vee/B}\right),$$

where Y^{univ} is the universal vector extension of Y.

Theorem 4 (Gao)**.** ([5]) Use the notation above. Then $Y^\natural$ is bi-algebraic iff

(1) Y is bi-algebraic;

(2) $Y^\natural = Y^{univ} \times_B \mathbb{V}^\dagger \times_B (L \times B)$, where $\mathbb{V}^\dagger$ is an automorphic subbundle of $\left(\omega_{\pi^{-1}(B)^\vee/B}/\omega_{Y^\vee/B}\right)$ and L is an irreducible subvariety of a fiber of $\mathbb{C}_B^k \to B$ (here $\mathbb{C}_B^k$ is the largest trivial automorphic subbundle of $\left(\omega_{\pi^{-1}(B)^\vee/B}/\omega_{Y^\vee/B}\right)$).

3. Some transcendental statements

We have some transcendental results for $\mathfrak{A}_g^\natural$. See [5].

Theorem 5 (logarithmic Ax)**.** Let $Y^\natural$ be an irreducible subvariety of $\mathfrak{A}_g^\natural$. Let $\tilde{Y}^\natural$ be a complex analytic irreducible component of $\mathrm{unif}^{-1}(Y^\natural)$ and let $\tilde{Y}^{\natural,Zar}$ be its Zariski closure in $\mathbb{C}^{2g} \times \mathcal{H}_g^+$. Then $\tilde{Y}^{\natural,Zar}$ is bi-algebraic.

Theorem 6 (Ax-Lindemann)**.** Let $\tilde{Z}^\natural$ be an algebraic subset of $\mathbb{C}^{2g} \times \mathcal{H}_g^+$, then any irreducible component of $\mathrm{unif}(\tilde{Z}^\natural)^{Zar}$ is bi-algebraic.

Conjecture 1 (weak Ax-Schanuel)**.** Let $\tilde{Z}^\natural$ be a complex analytic irreducible subvariety of $\mathbb{C}^{2g} \times \mathcal{H}_g^+$. Let $\tilde{X}^\natural := (\tilde{Z}^\natural)^{\mathrm{Zar}}$ and let $Y^\natural := \mathrm{unif}(\tilde{Z}^\natural)^{\mathrm{Zar}}$. Let $F^\natural$ be the smallest bi-algebraic subvariety of $\mathfrak{A}_g^\natural$ containing $\mathrm{unif}(\tilde{Z}^\natural)$. Then $\dim \tilde{X}^\natural + \dim Y^\natural - \dim \tilde{Z}^\natural \geqslant \dim F^\natural$.

The weak Ax-Schanuel conjecture implies both logarithmic Ax and Ax-Lindemann. We also have an Ax-Schanuel conjecture, but we must introduce the weakly special part of an arbitrary bi-algebraic subvariety of $\mathfrak{A}_g^\natural$ in order to give the statement. We omit it here, but refer to [5]. For relative version of these results (i.e. the bi-algebraic system given in (1)), we refer to Bertrand-Pillay [1, 2].

References

[1] D. Bertrand and A. Pillay. A Lindemann-Weierstrass theorem for semi-abelian varieties over function fields. *J.Amer.Math.Soc.*, 23(2):491–533, 2010.

[2] D. Bertrand and A. Pillay. Galois theory, functional Lindemann–Weierstrass, and Manin maps. *Pacific Journal of Mathematics*, 281:51–82, 2016.

[3] Z. Gao. Towards the André-Oort conjecture for mixed Shimura varieties: the Ax-Lindemann-weierstrass theorem and lower bounds for Galois orbits of special points. *J.Reine Angew. Math (Crelle)*, online, 2015.

[4] Z. Gao. A special point problem of André-Pink-Zannier in the universal family of abelian varieties. *Annali della Scuola Normale Superiore di Pisa, Classe di Scienze*, to appear.

[5] Z. Gao. Enlarged mixed Shimura varieties, bi-algebraic system and some Ax type transcendental results. *Preprint*, available on the author's page, 2015.

[6] H. Shiga and J. Wolfart. Criteria for complex multiplication and transcendence properties of automorphic functions. *J.Reine Angew. Math (Crelle)*, 463:1–25, 1995.

[7] E. Ullmo. Structures spéciales et problème de Pink-Zilber. *Panoramas et Synthèses*, to appear.

[8] G. Wüstholz. Algebraic groups, Hodge theory, and transcendence. In *Proceedings of the International Congress of Mathematicians*, volume 1,2, pages 476–483, 1986.

Height bounds for algebraic numbers under splitting conditions

Lukas Pottmeyer
(joint work with Paul Fili)

Let h be the absolute logarithmic Weil height on a fixed algebraic closure $\overline{\mathbb{Q}}$ of the rational numbers $\mathbb{Q}$. It is well known that there are only finitely many algebraic numbers of bounded height and bounded degree. This result is commonly known as Northcott's theorem. In particular, there is a function $C : \mathbb{N} \to \mathbb{R}_{>0}$ such that for all $\alpha \in \overline{\mathbb{Q}}$ of degree $\deg(\alpha) \leq d$ we have $h(\alpha) \geq C(d)$ or $h(\alpha) = 0$.

A strong version of the Lehmer conjecture predicts that $C(d) = \frac{\log \ell}{d}$, where $\ell = 1.176280...$ is the Lehmer constant; i.e. the largest real root of the polynomial $x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$. So far the best known valid choice for $C(d)$ is a result of Dobrowolski [2] slightly strengthened by Voutier [6]:

$$C(d) = \frac{1}{4d} \left(\frac{\log \log d}{\log d} \right)^3 . \tag{1}$$

We give an effective lower bound for the height of an algebraic number $\alpha \in \overline{\mathbb{Q}}$ depending only on the splitting behaviour of the rational primes $M_{\mathbb{Q}}$ (including the archimedean prime ∞) in the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$.

For the rest of this text we fix a non-empty subset $S \subseteq M_{\mathbb{Q}}$. Our result merges two results due to Schinzel [5], and Bombieri and Zannier [1]:

Theorem 1 (Schinzel)**.** Let $\alpha \in \overline{\mathbb{Q}} \setminus \{0, \pm 1\}$ be totally real, which means that ∞ splits completely in $\mathbb{Q}(\alpha)$, then $h(\alpha) \geq \frac{1}{2} \log \left(\frac{\sqrt{5}+1}{2} \right)$.

Theorem 2 (Bombieri and Zannier)**.** Let $\alpha \in \overline{\mathbb{Q}}$ be such that p splits completely in $\mathbb{Q}(\alpha)$ for all $p \in S \setminus \{\infty\}$. There is an effectively given function $F : \mathbb{N} \to \mathbb{R}$ depending only on S such that

(1) $h(\alpha) \geq F(\deg(\alpha))$
(2) $F(d) \longrightarrow \frac{1}{2} \sum_{p \in S \setminus \{\infty\}} \frac{\log p}{p+1}$ as d tends to infinity.

Finally our result reads:

Theorem 3. Let $\alpha \in \overline{\mathbb{Q}}$ be such that p splits completely in $\mathbb{Q}(\alpha)$ for all $p \in S$. There is an effectively given function $F : \mathbb{N} \to \mathbb{R}$ depending only on S such that

(1) $h(\alpha) \geq F(\deg(\alpha))$
(2) $F(d) \longrightarrow \frac{1}{2} \sum_{p \in S \setminus \{\infty\}} \frac{p \log p}{p^2 - 1} + \sum_{p \in S \cap \{\infty\}} \frac{7\zeta(3)}{4\pi^2}$ as d tends to infinity.

Here, ζ denotes the Riemann zeta function.

The existence of the function F from Theorem 3 was already proven by Fili and Petsche [4]. Note that the constant $\frac{7\zeta(3)}{4\pi^2} = 0.213139...$ is not too much smaller than Schinzel's bound $\frac{1}{2} \log \left(\frac{\sqrt{5}+1}{2} \right) = 0.240605....$ In both of the Theorems 2 and 3 one gets a similar result when the ramification and inertia indices for $p \in S \setminus \{\infty\}$ in $\mathbb{Q}(\alpha)/\mathbb{Q}$ are bounded by any constants e_p and f_p. (In the formulation I chose for this presentation we obviously have $e_p = f_p = 1$.)

Combining the function F with the bound in (1) gives explicit lower bounds for algebraic numbers α as in Theorem 3. For instance, if $S = \{2, 3\}$, then $h(\alpha) = 0$ or $h(\alpha) \geq \frac{\log 2}{11}$ for all α such that 2 and 3 are totally split in $\mathbb{Q}(\alpha)$.

The idea for the proof of our theorem is to use potential theory on the Berkovich projective line $\mathbb{P}_p^{1,Berk}$. For $p = \infty$ the Berkovich line is nothing but $\mathbb{P}^1(\mathbb{C})$. For $p < \infty$ it is a path-connected Hausdorff space, which contains $\mathbb{P}^1(\mathbb{C}_p)$ as a dense subspace.

The bridge between height theory and Berkovich spaces is given by a result of Favre and Rivera-Letelier [3], that the height of any algebraic number α can be presented by

(2)
$$h(\alpha) = \frac{1}{2} \sum_{p \in M_{\mathbb{Q}}} \iint_{(\mathbb{P}_p^{1,Berk})^2 \setminus \{(z,z) | z \in \mathbb{P}^1(\mathbb{C}_p)\}} -\log |x-y|_p \mathrm{d}([\alpha]-\lambda_p)(x) \mathrm{d}([\alpha]-\lambda_p)(y).$$

Here, $[\alpha]$ is the probability measure on $\mathbb{P}_p^{1,Berk}$, which is equally supported on the Galois-conjugates of α, and λ_p is a canonical measure on $\mathbb{P}_p^{1,Berk}$ resembling the Haar-measure on the complex unit circle.

We approximate $h(\alpha)$ with a formula of the form (2) where $[\alpha]$ is replaced by a probability measure without point-masses. Hence, we do not have to exclude the diagonal in the remaining integral. This enables us to apply analytic tools like (a non-archimedean version) of Frostman's theorem, to estimate this integral. As all our calculations are explicit, we achieve an effective lower bound for $h(\alpha)$ with the properties stated in Theorem 3.

References

[1] 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.

[2] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), 391–401.

[3] C. Favre and J. Rivera-Letelier, *Équidistribution quantitative des points de petite hauteur sur la droite projective*, Math. Ann. **335** (2006), 311–361.

[4] P. Fili and C. Petsche, *Energy integrals over local fields and global height bounds*, Int. Math. Res. Not. IMRN 2015 no. 5, 1278–1294.

[5] A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number*, Acta Arith. **24** (1973), 385–399.

[6] P. Voutier, *An effective lower bound for the height of algebraic numbers*, Acta Arith **74** (1996), 81–95.

Compositional analogs of the Bugeaud-Corvaja-Zannier theorem, and applications

Thomas J. Tucker

In 2003, Bugeaud, Corvaja, and Zannier [BCZ03] proved the following theorem.

Theorem 1. Let a and b be two positive integers that are multiplicatively independent (i.e., there are no positive integers m and n such that $a^m = b^n$). Let $\epsilon > 0$. Then for all n, we have

$$\gcd(a^n - 1, b^n - 1) \ll \exp(\epsilon n).$$

The core of the proof is a delicate use of the Schmidt subspace theorem.

Later, Ailon and Rudnick [AR04] showed that something even stronger holds over function fields, specifically the following.

Theorem 2. Let $a, b \in \mathbb{C}[x]$ be two non constant, multiplicatively independent polynomials. Then there is a polynomial h such that for any integer n, we have

$$\gcd(a^n - 1, b^n - 1) | h.$$

The proof they gave is quite simple. If $(x - \lambda)$ divides $\gcd(a^n - 1, b^n - 1)$ (for $\lambda \in \mathbb{C}$), then $a(\lambda)$ and $b(\lambda)$ are both roots of unity. By the Serre-Ihara-Tate theorem see [Lan65]), the parametrized curve $(a(t), b(t))$ can only contain infinitely many roots of unity if a and b are multiplicatively dependent. We note here that one need not worry about the multiplicities of the $(x-\lambda)$ dividing $\gcd(a^n-1, b^n-1)$ here since they cannot increase as n increases for elementary reasons.

Ostafe asked whether one could prove a "compositional version" of the Ailon-Rudnick theorem, where instead of working with multiplicative powers a^n, one works instead with compositional powers $f^{\circ n}$ for a polynomial f. Here, the notion of dependence becomes a bit more complicated, since one cannot use the naïve notion involving equality of powers. The reason for this is that composition is not a commutative operation. Instead, we use this definition.

Definition 1. Let f and g be two non constant polynomials. We say that f and g are compositionally dependent if there is a polynomial h and a linear polynomial σ of finite compositional order such that any compositional product

$$f^{\circ i_1} g^{\circ j_1} \circ \cdots \circ f^{\circ i_n} g^{\circ j_n}$$

(where the i_r and j_s are nonnegative integers) is equal to $\sigma^{\circ k} \circ h^{\circ \ell}$ for some nonnegative integers k and ℓ.

One other difference in the compositional case is the possibility of increasing multiplicity for factors of $\gcd(f^{\circ n} - c, g^{\circ n} - c)$. This happens for example if $c = 0$, and f and g are both divisible by x^2. Thus, we need one more definition: we say that c is in a ramified cycle of a polynomial q if there is a positive integer n such that $q^{\circ n}(c) = c$ and $(q^{\circ n})'(c) = 0$.

With these definitions we are ready to state a compositional analog of the Ailon-Rudnick theorem. This theorem represents joint work with Liang-Chung Hsia.

Theorem 3. Let $f, g \in \mathbb{C}[x]$ be two compositionally independent polynomials, at least one of which is not conjugate to a monomial in x or a Chebychev polynomial. Suppose that $c \in \mathbb{C}[x]$ is not in a ramified cycle for f or g. Then there is a polynomial h such that for all n, we have

$$\gcd(f^{\circ n} - c, g^{\circ n} - c) | h.$$

The proof uses some (now standard) ideas from equidistribution. Using Silverman specialization and equidistribution of points with small height, we can show that if there are infinitely many λ such that $(x - \lambda)$ divides $\gcd(f^{\circ n} - c, g^{\circ n} - c)$ for some n, then the canonical heights for f and g are the same, which forces the Julia sets of f and g to be the same. Work of Beardon [Bea90, Bea90], Schmidt, and Steinmetz [SS95] then shows that f and g must be multiplicatively dependent.

Proving a compositional version of the Bugeaud-Corvaja-Zannier theorem over number fields seems more difficult. However, following an idea of Silverman [Sil05], if one assumes a conjecture of Vojta [Voj87] in special case of heights of points with respect to the canonical divisor on blow-ups of $\mathbb{P}^2$, then one can prove such a result, though with a somewhat unsatisfactory definition of compositional independence. This represents work in progress due to Keping Huang.

One of our main reasons for studying these questions is to begin a possible classification of all iterated Galois groups of polynomials over number fields. Let f be a rational function over a number field K. For each n, let $K_n = K(f^{-\circ n}(0))$, let G_n denote the Galois group of K_n over K, and let G denote the inverse limit of the G_n. Motivated by questions of Boston and Jones, we hope to come up with a conjectural classification of all possible G that arise in this way. Assuming the Vojta conjecture for rational points on surfaces along with a conjecture about the irreducibility of iterates $f^{\circ n}$ (subject to the condition that 0 is not periodic under f), we believe, jointly with Andrew Bridy, that we can carry out this classification completely for quadratic rational functions over number fields, building on work of Pink. The idea here is that Galois groups come from ramification groups and ramification groups come from the orbits of critical points modulo primes. Control of $\gcd(f^{\circ n}(\alpha), f^{\circ n}(\beta))$, for α and β the critical points of f, allows one to control the Galois groups G_n.

References

[AR04] N. Ailon and Z. Rudnick, *Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$*, Acta Arith. **113** (2004), no. 1, 31–38.

[BCZ03] Y. Bugeaud, P. Corvaja, and U. Zannier, *An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$*, Math. Z. **243** (2003), no. 1, 79–84.

[Bea90] A. F. Beardon, *Symmetries of Julia sets*, Bull. London Math. Soc. **22** (1990), no. 6, 576–582.

[Bea92] ———, *Polynomials with identical Julia sets*, Complex Variables Theory Appl. **17** (1992), no. 3-4, 195–200.

[Lan65] S. Lang, *Division points on curves*, Ann. Mat. Pura Appl. (4) **70** (1965), 229–234.

[Sil05] J. H. Silverman, *Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups*, Monatsh. Math. **145** (2005), no. 4, 333–350.

[SS95] W. Schmidt and N. Steinmetz, *The polynomials associated with a Julia set*, Bull. London Math. Soc. **27** (1995), no. 3, 239–241.

[Voj87] P. Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Mathematics, vol. 1239, Springer-Verlag, Berlin, 1987.

Property (N), Decidability and Diophantine Approximation

Martin Widmer

In this report we discuss a connection, recently observed by Vidaux and Videla, between the undecidability of certain rings of algebraic numbers and Property (N), as well as possible values for the Northcott number of a ring.

Throughout this note K denotes a subfield of the algebraic numbers $\overline{\mathbb{Q}}$, and $\mathcal{O}_K$ denotes the ring of integers of K. We write $K^{(d)}$ for the composite field of all extensions of K of degree at most d, $K_{ab}^{(d)}$ for the maximal abelian subextension of $K^{(d)}/K$, and K_{tr} for the maximal totally real subfield of K.

Let $H(\cdot)$ denote the absolute multiplicative Weil height on $\overline{\mathbb{Q}}$. Following Bombieri and Zannier we say a subset A of $\overline{\mathbb{Q}}$ has Property (N) if for every $X \geq 1$

$$|\{\alpha \in A; H(\alpha) \leq X\}| < \infty.$$

Northcott already back in 1949 showed that number fields have Property (N). In 2001 Bombieri and Zannier [1] asked which other fields have Property (N). This is a difficult widely open problem, but here are some examples.

Theorem 1 (Bombieri, Zannier 2001)**.** Let k be a number field, and let d be a positive integer. Then $k_{ab}^{(d)}$ has Property (N).

Another criterion was given by the author in 2011.

Theorem 2 ([7])**.** Let k be a number field, let $k = k_0 \subsetneq k_1 \subsetneq k_2 \subsetneq \dots$ be a nested sequence of finite extensions, and set $K = \bigcup_i k_i$. Suppose that

$$\inf_{k_{i-1} \subsetneq M \subseteq k_i} \left(\frac{|\Delta_M|^{\frac{1}{[M:k_{i-1}]}}}{|\Delta_{k_{i-1}}|} \right)^{\frac{1}{[M:k_0]}} \longrightarrow \infty$$

as i tends to infinity where the infimum is taken over all intermediate fields M strictly larger than k_{i-1}, and Δ_{k_i} denotes the discriminant of k_i. Then the field K has Property (N).

In particular, for $d_i \in \mathbb{N}$ the field $\mathbb{Q}(2^{1/d_1}, 3^{1/d_2}, 5^{1/d_3}, 7^{1/d_4}, \dots)$ has Property (N) if and only if the sequence $(\log 2)/d_1, (\log 3)/d_2, (\log 5)/d_3, (\log 7)/d_4, \dots$ tends to infinity (cf. [7]).

We say an enumerable ring R is decidable if its full first order theory in the language $\mathcal{L} = (\cdot, +, -, 0, 1)$ of rings is decidable. If R is not decidable we say R is undecidable. Gödel has shown that $\mathbb{Z}$ is undecidable. By showing that $\mathbb{Z}$ is definable in R by a first order formula (from now on we drop "by a first order formula") J.Robinson [2, 3] has shown that number fields, their ring of integers, $\mathcal{O}_{\mathbb{Q}_{tr}^{(2)}}$, and $\mathcal{O}_{\overline{\mathbb{Q}}_{tr}}$ are all undecidable. Interestingly $\overline{\mathbb{Q}}_{tr}$ is decidable as shown by

Fried, Haran and Völklein. Other examples of decidable subrings of $\overline{\mathbb{Q}}$ are $\mathcal{O}_{\overline{\mathbb{Q}}}$ (van den Dries) and $\overline{\mathbb{Q}}$ (Tarski).

For a totally real ring $\mathcal{O} \subset \overline{\mathbb{Q}}$ Julia Robinson [3] considered the quantity

$$JR(\mathcal{O}) = \inf_{t\in\mathbb{R}} \{t; |\{\alpha \in \mathcal{O}; 0 \ll \alpha \ll t\}| = \infty\}$$

where $0 \ll \alpha \ll t$ means $0 < \sigma(\alpha) < t$ for all conjugates $\sigma(\alpha)$ over $\mathbb{Q}$.

Only little is known about the possible values of $JR(\cdot)$ (see, e.g., [4]). Following Vidaux and Videla [4] we say that $\mathcal{O}$ has Property (JR) if either $JR(\mathcal{O}) = \infty$ or the infimum is attained.

Theorem 3 (J. Robinson 1962)**.** Let K be a totally real subfield of $\overline{\mathbb{Q}}$ and suppose $\mathcal{O}_K$ has Property (JR). Then $\mathbb{Z}$ is definable in $\mathcal{O}_K$ and hence $\mathcal{O}_K$ is undecidable.

This criterion allowed her to deduce the following result.

Corollary 1 (J. Robinson 1962)**.** Let $K = \mathbb{Q}_{tr}^{(2)} = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \ldots)$. Then $\mathcal{O}_K$ is undecidable.

Videla [6] has shown that if $\mathcal{P}$ is a finite set of rational primes and $K/\mathbb{Q}$ is a pro-$\mathcal{P}$ Galois extension then $\mathcal{O}_K$ is definable in K. In particular, $\mathcal{O}_{\mathbb{Q}_{tr}^{(d)}}$ is definable in $\mathbb{Q}_{tr}^{(d)}$. As $\mathcal{O}_{\mathbb{Q}_{tr}^{(2)}}$ is undecidable it follows that $\mathbb{Q}_{tr}^{(2)}$ is undecidable.

Theorem 4 (Vidaux, Videla 2016)**.** If K is a totally real subfield of $\overline{\mathbb{Q}}$ and $\mathcal{O}_K$ has Property (N) then $\mathcal{O}_K$ has Property (JR). In particular, $\mathcal{O}_K$ is undecidable.

The proof of this interesting observation is an immediate consequence of Theorem 3: if $t > 1$ and α is a totally real algebraic integer with $0 \ll \alpha \ll t$ then $H(\alpha) < t$. In particular, $JR(\mathcal{O}) = \infty$ whenever $\mathcal{O}$ has Property (N). Let $d > 2$ be an integer. Already Bombieri and Zannier [1] asked whether $\mathbb{Q}^{(d)}$ has Property (N). This remains a difficult open question; but to show that $\mathcal{O}_{\mathbb{Q}_{tr}^{(d)}}$ and $\mathbb{Q}_{tr}^{(d)}$ are both undecidable it would suffice to have an affirmative answer to the following question.

Question 1. Does $\mathcal{O}_{\mathbb{Q}_{tr}^{(d)}}$ have Property (N)?

Inspired by J. Robinson's quantity $JR(\cdot)$ Vidaux and Videla [4] introduced the Northcott number $N(\mathcal{O})$ of a subring $\mathcal{O}$ of $\overline{\mathbb{Q}}$ defined by

$$N(\mathcal{O}) = \inf_{t\in\mathbb{R}} \{t; |\{\alpha \in \mathcal{O}; H(\alpha) < t\}| = \infty\},$$

and they proposed the following question.

Question 2 (Vidaux, Videla 2016)**.** Which real numbers can be realised as Northcott numbers of subrings of $\overline{\mathbb{Q}}$?

Using arguments from the proof of Theorem 2 one can easily show:

Theorem 5. For any $A \geq 1$ there exists a field $K \subset \overline{\mathbb{Q}}$ with

$$A \leq N(K) \leq N(\mathcal{O}_K) \leq A^2.$$

References

[1] E. Bombieri and U. Zannier, *A Note on heights in certain infinite extensions of* $\mathbb{Q}$, Rend. Mat. Acc. Lincei, **12** (2001), 5–14.

[2] J. Robinson, *The undecidability of algebraic rings and fields*, Proc. Amer. Math. Soc. **10** (1959) 950–957.

[3] J. Robinson, *On the decision problem for algebraic rings*, in Studies in Mathematical Analysis and Related Topics, ed. by G. Szeg (Stanford University Press, Stanford, 1962), 297–304.

[4] X. Vidaux and C. R. Videla, *Definability of the natural numbers in totally real towers of nested square roots*, Proc. Amer. Math. Soc. **48** (1) (2016), 58–62.

[5] X. Vidaux and C. R. Videla, *A note on the Northcott property and undecidability*, Bull. London Math. Soc. **143** (10) (2015), 4463–4477.

[6] C. R. Videla, *Definability of the ring of integers in pro-p Galois extensions of number fields*, Israel J. Math. **118** (2000), 1–14.

[7] M. Widmer, *On certain infinite extensions of the rationals with Northcott property*, Monatsh. Math. **162** (3) (2011), 341–353.

Pell's equation in polynomials and additive extensions

Harry Schmidt

We study certain one-parameter families of Pell's equations in polynomials with a triple zero. The main interest lies in the relation between the generic equation and its various specializations.

For polynomials of degree 6 with a double zero such a study was undertaken by Bertrand [B2]. For example, he considered

$$A^2 - DB^2 = 1, B \neq 0 \tag{1}$$

$$D = (X + 1/2)^2(X^4 + X + t) \tag{2}$$

and showed that there are only finitely many $t \in \mathbb{C}$ such that the above system (1), (2) has a solution with $A, B \in \mathbb{C}[X]$ (Corollary 2, p.14). Necessarily (1), (2) is not solvable with $A, B \in \overline{\mathbb{C}(t)}[X]$ and t generic over $\mathbb{C}$. Since then infinitely many specializations of A, B would lead to a solution of the specialized equation.

However, he also showed that although (1) does not have a generic solution for

$$D = X^2(X^2 - 1)(X^2 + tX + 1)$$

there are infinitely many specializations that do have a solution (Corollary 3, p.20). As explained in [B2] this exceptional behavior arises from special curves in semi-constant families of multiplicative extensions. The above example is directly connected to the delicate Ribet curves. (See also [B1].)

When D is of degree 6 and has no zeros of multiplicity higher than 1 we are led to study families of abelian varieties of relative dimension 2. Here Masser and Zannier have shown that for

$$D = X^6 + X + t$$

(1) is solvable for at most finitely many $t \in \mathbb{C}$ while for

$$D = X^6 + X^2 + t$$

there are infinitely many $t \in \mathbb{C}$ such that (1) is solvable although the generic equation is not (see [Za, p.86/87]).

The proof of the above statement goes by considering a section of a family of algebraic groups over a curve of relative dimension 2 and intersecting its image with the image of all torsion sections. For the right choice of a section the finiteness of this intersection implies the same for the set of t for which (1) is solvable. Conversely if the intersection is infinite we can deduce infiniteness for this set of t.

When the section under study is not special this intersection should be finite. The first result in this direction is the by-now classical $2,3$-example in [MZ1] where much of the groundwork for subsequent results such as [BMPZ], [MZ2], [MZ3] and [MZ4] was laid out.

When the algebraic group under study is a non-split additive extension of an elliptic family there are essentially no dangerous special sub-varieties except for the torsion sections. As this is the group that arises in the study of polynomials of degree 6 with a triple zero we can show the following.

Theorem 1. Let $\mathcal{K} = \mathbb{C}(\mathcal{V})$ be the function field of a curve $\mathcal{V}$ and let $D \in \mathcal{K}[X]$ be of degree 6 with a triple zero (in $\overline{\mathcal{K}}$). If (1) has no solution with $A, B \in \overline{\mathcal{K}}[X]$ then there are at most finitely many $v \in \mathcal{V}(\mathbb{C})$ such that (1) has a solution for the specialization $D_v \in \mathbb{C}[X]$ (and $A, B \in \mathbb{C}[X]$).

Note that in view of the results mentioned above we cannot remove the condition on D to have a triple zero.

References

[B1] D. Bertrand (with an Appendix by Bas Edixhoven), *Special points and Poincaré bi-extensions*, arXiv:1104.5178, (11 pages).

[B2] D. Bertrand, *Generalized jacobians and Pellian polynomials*, to appear in J. Th. Nombres Bordeaux.

[BMPZ] D. Bertrand, D. Masser, A. Pillay, U. Zannier, *Relative Manin-Mumford for semi-abelian surfaces*, accepted in Proc. Edinburgh Math. Soc.

[MZ1] D. Masser, U. Zannier, *Torsion anomalous points and families of elliptic curves*, American J. Math. 132, 1677–1691 (2010).

[MZ2] D. Masser, U. Zannier, *Torsion points on families of squares of elliptic curves*, Math. Ann. 352, 453–484 (2012).

[MZ3] D. Masser, U. Zannier, *Torsion points on families of products of elliptic curves*, Adv. Math. 259, 116–133 (2014).

[MZ4] D. Masser, U. Zannier, *Torsion points on families of simple abelian surfaces and Pell s equation over polynomial rings (with Appendix by V. Flynn)*, to appear in J. European Math. Soc.

[Za] U. Zannier (with appendixes by David Masser), *Some Problems of Unlikely Intersections in Arithmetic and Geometry,* Annals of Mathematics Studies 181, Princeton University Press, Princeton, NJ (2012).

Remarks on the topology of Diophantine approximation Spectra

Damien Roy

Fix an integer $n \geq 2$. To each non-zero point $\mathbf{u}$ in $\mathbb{R}^n$, one attaches several numbers called *exponents of Diophantine approximation*. However, as Khintchine first observed, these numbers are not independent of each other. This raises the problem of describing the set of all possible values that a given family of exponents can take by varying the point $\mathbf{u}$. To avoid trivialities, one restricts to points $\mathbf{u}$ whose coordinates are linearly independent over $\mathbb{Q}$. The resulting set of values is called the *spectrum of these exponents*. We show that, in an appropriate setting, any such spectrum is a compact connected set. In the case $n = 3$, we prove moreover that it is closed under a simple binary operation. For $n = 3$, we also obtain a description of the spectrum of the exponents $(\underline{\varphi}_1, \underline{\varphi}_2, \underline{\varphi}_3, \bar{\varphi}_1, \bar{\varphi}_2, \bar{\varphi}_3)$ recently introduced by Schmidt and Summerer.

1. A quick survey

Fix an integer $n \geq 2$ and a non-zero point $\mathbf{u} \in \mathbb{R}^n$. Then, consider the parametric family of convex bodies of $\mathbb{R}^n$ given by

$$\mathcal{C}_{\mathbf{u}}(q) = \{\mathbf{x} \in \mathbb{R}^n \,;\, \|\mathbf{x}\| \leq 1 \text{ and } |\mathbf{x} \cdot \mathbf{u}| \leq e^{-q}\} \quad (q \geq 0),$$

where $\mathbf{x}\cdot\mathbf{u}$ denotes the standard scalar product of $\mathbf{x}$ and $\mathbf{u}$ in $\mathbb{R}^n$, and $\|\mathbf{x}\| = |\mathbf{x}\cdot\mathbf{x}|^{1/2}$ is the Euclidean norm of $\mathbf{x}$. For each $i = 1, \ldots, n$ and each $q \geq 0$, set

$$L_{\mathbf{u},i}(q) = \log \lambda_i(\mathcal{C}_{\mathbf{u}}(q), \mathbb{Z}^n)$$

where $\lambda_i(\mathcal{C}_{\mathbf{u}}(q), \mathbb{Z}^n)$ is the i-th minimum of $\mathcal{C}_{\mathbf{u}}(q)$ with respect to the lattice $\mathbb{Z}^n$, namely the smallest positive real number λ such that $\lambda\mathcal{C}_{\mathbf{u}}(q)$ contains at least i linearly independent points of $\mathbb{Z}^n$. In 1982, using a slightly different but equivalent setting, Schmidt noted that, for the purpose of Diophantine approximation, it would be important to understand the behavior of the maps $\mathbf{L}_{\mathbf{u}} \colon [0, \infty) \to \mathbb{R}^n$ given by

$$\mathbf{L}_{\mathbf{u}}(q) = (L_{\mathbf{u},1}(q), \ldots, L_{\mathbf{u},n}(q)) \quad (q \geq 0)$$

(see [16]). Transposed to the present setting, his preliminary observations can be summarized as follows. We have $L_{\mathbf{u},1}(q) \leq \cdots \leq L_{\mathbf{u},n}(q)$ for each $q \geq 0$ and, by Minkowski's second convex body theorem, the function $L_{\mathbf{u},1}(q) + \cdots + L_{\mathbf{u},n}(q) - q$ is bounded on $[0, \infty)$. Moreover, each $L_{\mathbf{u},i}$ is a continuous piecewise linear map with slopes 0 and 1. In the same paper [16], he also made a conjecture which was solved by Moshchevitin [11] (see also [9]).

In [17, 18], Schmidt and Summerer establish further properties of the map $\mathbf{L}_{\mathbf{u}}$ which, by work of the author [13], completely characterize these functions within the set of all functions from $[0, \infty)$ to $\mathbb{R}^n$, modulo bounded functions. They also introduce the quantities

$$\underline{\varphi}_i(\mathbf{u}) = \liminf_{q\to\infty} \frac{1}{q} L_{\mathbf{u},i}(q), \quad \bar{\varphi}_i(\mathbf{u}) = \limsup_{q\to\infty} \frac{1}{q} L_{\mathbf{u},i}(q) \quad (1 \leq i \leq n).$$

Revisiting work of Schmidt in [15], Laurent [8] defines additional exponents of approximation related to

$$\underline{\psi}_i(\mathbf{u}) = \liminf_{q\to\infty} \frac{1}{q} \sum_{j=1}^{i} L_{\mathbf{u},j}(q), \quad \bar{\psi}_i(\mathbf{u}) = \limsup_{q\to\infty} \frac{1}{q} \sum_{j=1}^{i} L_{\mathbf{u},j}(q) \quad (1 \le i < n).$$

Of particular interest are the exponents $\underline{\varphi}_1 = \underline{\psi}_1$, $\bar{\varphi}_1 = \bar{\psi}_1$, $\underline{\varphi}_n = -\bar{\psi}_{n-1}$ and $\bar{\varphi}_n = -\underline{\psi}_{n-1}$. Their spectrum is easily described for $n = 2$. For $n = 3$, it was computed by Laurent in [7]. In this case and in all cases where we know the spectrum of a family of m exponents, it happens to be a semi-algebraic subset of $\mathbb{R}^m$ defined over $\mathbb{Q}$, that is a subset of $\mathbb{R}^m$ defined by polynomial inequalities with rational coefficients. The spectra of the following general families are known:

- $(\underline{\varphi}_1, \bar{\varphi}_n)$: the contraints come from Khintchine's transference principle [5, 6], and constructions of Jarník in [2, 3] show that they are optimal,
- $(\underline{\psi}_1, \underline{\psi}_2, \dots, \underline{\psi}_{n-1})$: the constraints by Schmidt [15] and Laurent [8] describe the full spectrum [14],
- $(\bar{\varphi}_1, \underline{\varphi}_n)$: the contraints by Jarník [4] for $n = 3$, and by German [1] for $n \ge 4$ are optimal (Schmidt and Summerer [20]) and describe the full spectrum (Marnat [10]).

For $n = 4$, we also know optimal constraints on the spectrum of $(\underline{\varphi}_n, \bar{\varphi}_n)$ thanks to [12] and [19], as well as for the spectrum of $(\underline{\varphi}_1, \bar{\varphi}_1)$ thanks to [19].

2. Three new results

Theorem 1. Let $T = (T_1, \dots, T_m) \colon \mathbb{R}^n \to \mathbb{R}^m$ be a linear map, and let $\mathrm{Im}^*(\mu_T)$ denote the set of all m-tuples

$$\mu_T(\mathbf{L}_\mathbf{u}) = \Big(\liminf_{q\to\infty} q^{-1} T_1(\mathbf{L}_\mathbf{u}(q)), \dots, \liminf_{q\to\infty} q^{-1} T_m(\mathbf{L}_\mathbf{u}(q)) \Big)$$

where $\mathbf{u}$ is a point of $\mathbb{R}^n$ with $\mathbb{Q}$-linearly independent coordinates. Then $\mathrm{Im}^*(\mu_T)$ is a compact connected subset of $\mathbb{R}^m$.

For example, the spectrum of the exponents $(\underline{\varphi}_1, \dots, \underline{\varphi}_n, \bar{\varphi}_1, \dots, \bar{\varphi}_n)$ is the following set $\{T(\mathbf{x})\,;\, \mathbf{x} \in \mathrm{Im}^*(\mu_T)\}$ where $T \colon \mathbb{R}^n \to \mathbb{R}^{2n}$ is the linear map given by $T(\mathbf{x}) = (\mathbf{x}, -\mathbf{x})$ for any $\mathbf{x} \in \mathbb{R}^n$. Thus, that spectrum is compact and connected. By a similar reasoning, the same apply to the spectrum of $(\underline{\psi}_1, \dots, \underline{\psi}_{n-1}, \bar{\psi}_1, \dots, \bar{\psi}_{n-1})$.

It is useful to dispose of an alternative definition for $\mu_T(\mathbf{L}_\mathbf{u})$, using the coordinatewise partial ordering on $\mathbb{R}^m$. For this ordering, any bounded subset F of $\mathbb{R}^m$ has a greatest lower bound denoted $\inf(F)$. Then, in the notation of Theorem 1, we have

$$\mu_T(\mathbf{L}_\mathbf{u}) = \inf T(\mathcal{F}(\mathbf{L}_\mathbf{u})) = \big(\inf T_1(\mathcal{F}(\mathbf{L}_\mathbf{u})), \dots, \inf T_m(\mathcal{F}(\mathbf{L}_\mathbf{u})) \big),$$

where $\mathcal{F}(\mathbf{L_u})$ is the set of all $\mathbf{x} \in \mathbb{R}^n$ such that, for each $\epsilon > 0$, there are arbitrarily large positive real numbers q with $\|\mathbf{x} - q^{-1}\mathbf{L_u}(q)\|_\infty \le \epsilon$. More precisely, we have

$$\mu_T(\mathbf{L_u}) = \inf T(\mathcal{K}(\mathbf{L_u}))$$

where $\mathcal{K}(\mathbf{L_u})$ is the convex hull of $\mathcal{F}(\mathbf{L_u})$. When $n = 3$, we can show that, for any points $\mathbf{u}', \mathbf{u}'' \in \mathbb{R}^3$ with $\mathbb{Q}$-linearly independent coordinates, there exists a third point $\mathbf{u} \in \mathbb{R}^3$ of the same sort such $\mathcal{K}(\mathbf{L_u})$ is the convex hull of $\mathcal{K}(\mathbf{L_{u'}}) \cup \mathcal{K}(\mathbf{L_{u''}})$. This yields the following result.

Theorem 2. Suppose that $n = 3$, and let $T\colon \mathbb{R}^3 \to \mathbb{R}^m$ be a linear map. For any $\mathbf{x}, \mathbf{y}$ in $\mathrm{Im}^*(\mu_T)$, the point $\min(\mathbf{x}, \mathbf{y})$ also belongs to $\mathrm{Im}^*(\mu_T)$.

In fact, $\mathrm{Im}^*(\mu_T)$ contains the infimum of any of its subsets. It would be interesting to know if this property extends to dimension $n > 3$.

Theorem 3. Suppose that $n = 3$. Then the spectrum of $(\underline{\varphi}_1, \underline{\varphi}_2, \underline{\varphi}_3, \bar{\varphi}_1, \bar{\varphi}_2, \bar{\varphi}_3)$ is a semi-algebraic set defined over $\mathbb{Q}$ of dimension 5.

3. The main tool

Let $\mathbf{e}_1 = (1, 0, \dots, 0), \dots, \mathbf{e}_n = (0, \dots, 0, 1)$ denote the vectors of the canonical basis of $\mathbb{R}^n$. An *n-system* on $(0, \infty)$ is a continuous piecewise linear map $\mathbf{P} = (P_1, \dots, P_n)\colon (0, \infty) \to \mathbb{R}^n$ with the property that, for any $q > 0$,

- $0 \le P_1(q) \le \cdots \le P_n(q)$ and $P_1(q) + \cdots + P_n(q) = q$,
- there exist $k, \ell \in \{1, \dots, n\}$ such that $\mathbf{P}'(q^-) = \mathbf{e}_\ell$ and $\mathbf{P}'(q^+) = \mathbf{e}_k$,
- if $k > \ell$, then $P_\ell(q) = \cdots = P_k(q)$.

We say that such a map is *proper* if P_1 is unbounded. We say that it is *self-similar* if there exists a constant $\rho > 1$ such that $\mathbf{P}(\rho q) = \rho \mathbf{P}(q)$ for each $q > 0$.

It follows from [13, Theorem 1.3] that, modulo bounded functions, the classes of proper n-systems on $(0, \infty)$ are the same as the classes of the maps $\mathbf{L_u}$ restricted to $(0, \infty)$ where $\mathbf{u}$ runs through the elements of $\mathbb{R}^n$ with $\mathbb{Q}$-linearly independent coordinates. When $\mathbf{P}$ and $\mathbf{L_u}$ are in the same class, we have $\mathcal{F}(\mathbf{P}) = \mathcal{F}(\mathbf{L_u})$, $\mathcal{K}(\mathbf{P}) = \mathcal{K}(\mathbf{L_u})$, as well as $\mu_T(\mathbf{P}) = \mu_T(\mathbf{L_u})$ for any linear map $T\colon \mathbb{R}^n \to \mathbb{R}^m$, with the obvious definitions for $\mathcal{F}(\mathbf{P})$, $\mathcal{K}(\mathbf{P})$ and $\mu_T(\mathbf{P})$.

For T as above, we show that the points $\mu_T(\mathbf{P})$ with $\mathbf{P}$ proper and self-similar are dense in $\mathrm{Im}^*(\mu_T)$. The proofs of the results mentioned in Section 2 use this together with the construction of proper n-systems obtained by pasting pieces of other n-systems.

Acknowledgement. This research is partially supported by NSERC.

References

[1] O. N. German, Intermediate Diophantine exponents and parametric geometry of numbers, *Acta Arith.* **154** (2012), 79–101.

[2] V. Jarník, Über einen Satz von A. Khintchine, *Práce Mat.-Fiz.* **43** (1935), 151–166.

[3] V. Jarník, Über einen Satz von A. Khintchine II, *Acta Arith.* **2** (1936), 1–22.

[4] V. Jarník, Zum Khintchineschen "Übertragungssatz", *Trav. Inst. Math. Tbilissi* **3** (1938), 193–212.

[5] A. Y. Khintchine, Zur metrischen Theorie der diophantischen Approximationen, *Math. Z.* **24** (1926), 706–714.
[6] A. Y. Khintchine, Über eine Klasse linearer diophantischer Approximationen, *Rend. Circ. Math. Palermo* **50** (1926), 170–195.
[7] M. Laurent, Exponents of Diophantine approximation in dimension two, *Canad. J. Math.* **61** (2009), 165–189.
[8] M. Laurent, On transfer inequalities in Diophantine approximation, in: Analytic Number Theory in Honour of Klaus Roth, Cambridge U. Press (2009), 306–314.
[9] A. Keita, On a Conjecture of Schmidt for the Parametric Geometry of Numbers, *Mosc. J. Comb. Number Theory* **6** (2016), to appear.
[10] A. Marnat, About Jarník's-type relation in higher dimension, preprint, 22 pages.
[11] N. G. Moshchevitin, Proof of W. M. Schmidt's conjecture concerning successive minima of a lattice, *J. Lond. Math. Soc.* **86** (2012), 129–151.
[12] N. G. Moshchevitin, Exponents for three-dimensional simultaneous Diophantine approximations, *Czechoslovak Math. J.* **62** (2012), 127–137.
[13] D. Roy, On Schmidt and Summerer parametric geometry of numbers, *Ann. of Math.* **182** (2015), 739–786.
[14] D. Roy, Spectrum of the exponents of best rational approximation, *Math. Z.* **283** (2016), 143–155.
[15] W. M. Schmidt, On heights of algebraic subspaces and diophantine approximations, *Ann. of Math.* **85** (1967), 430–472.
[16] W. M. Schmidt, Open problems in Diophantine approximations, in: *Approximations diophantiennes et nombres transcendants* (Luminy 1982), Progr. Math., vol. 31, pp. 271–287, Birkhäuser, Boston, 1983.
[17] W. M. Schmidt and L. Summerer, Parametric geometry of numbers and applications, *Acta Arith.* **140** (2009), 67–91.
[18] W. M. Schmidt and L. Summerer, Diophantine approximation and parametric geometry of numbers, *Monatsh. Math.* **169** (2013), 51–104.
[19] W. M. Schmidt and L. Summerer, Simultaneous approximation to three numbers, *Mosc. J. Comb. Number Theory* **3** (2013), 84–107.
[20] W. M. Schmidt and L. Summerer, The generalization of Jarnik's identity, preprint, 17 pages.

Squares with three nonzero digits

Michael Bennett
(joint work with Adrian Scheerer)

Let us denote by $N_x(y)$ the number of nonzero digits in the base$-x$ representation of a positive integer y (where, say, $x > 1$ is an integer). Work of Hare, Laishram and Stoll [1] proves that, infinitely often, one has

$$\frac{N_x(y^2)}{N_x(y)} \leq \frac{\kappa}{\log y},$$

where $\kappa = \kappa(x)$. In the (very) special case that $N_x(y^2) = 3$, a result of Corvaja and Zannier [2], based upon Schmidt's Subspace Theorem, implies that, given x, there are at most finitely many y for which

$$\frac{N_x(y^2)}{N_x(y)} \leq 1.$$

The ineffectivity of the Subspace Theorem makes quantifying this statement rather challenging. In this talk, we describe how to do this for certain integers x with a large prime-power factor. We carry this out explicitly for $x \in \{2, 3, 4, 5, 8\}$. Our proofs rely upon the hypergeometric method, based upon Padé approximation to binomial functions.

References

[1] K. Hare, S. Laishram, T. Stoll, *Stolarsky's conjecture and the sum of digits of polynomial values*, Proc. Amer. Math. Soc. **139** (2011), 39–49.

[2] P. Corvaja and U. Zannier, *On the diophantine equation* $f(a^m, y) = b^n$, Acta Arith. **XCIV** (2000), 25–40.

An arithmetic dynamical analogue of the Mordell–Lang conjecture

Michael E. Zieve

(joint work with Trevor Hyde)

In recent years there has been much interest in arithmetic properties of points in an orbit of a rational function. Here for any rational function $f(X)$ with coefficients in a field K, we write $f^n(X)$ for the n-th iterate of $f(X)$, namely the n-fold composition $f \circ f \circ \cdots \circ f$. For $P \in K$, the orbit of P under $f(X)$ is the sequence of points $P, f(P), f^2(P), f^3(P), \ldots$. Recently Cahn, Jones and Spear made the following conjecture [5]:

Conjecture 1. For any field K of characteristic zero, any $u, f \in K(X)$ with $\deg(f) > 1$, and any $P \in K$, the set $\{n \in \mathbb{N} \colon f^n(P) \in u(K)\}$ is the union of finitely many sets of the form $a + b\mathbb{N}$ with $a, b \in \mathbb{Z}$.

Note that if $b = 0$ then $a + b\mathbb{N}$ consists of just the single integer a, so that any finite subset of $\mathbb{N}$ is allowed in the conclusion of Conjecture 1. We express the conclusion in words by saying that $\{n \in \mathbb{N} \colon f^n(P) \in u(K)\}$ is the union of finitely many one-sided arithmetic progressions. We first show that Conjecture 1 is false in general:

Proposition 1. Let $u(X) := X^2$ and $f(X) := X^2 - X + 1$, and define the field $K := \mathbb{Q}(\{\sqrt{f^{n^2}(2)} \colon n \in \mathbb{N}\})$. Then $\{n \in \mathbb{N} \colon f^n(2) \in u(K)\} = \{n^2 \colon n \in \mathbb{N}\}$, which is not the union of finitely many one-sided arithmetic progressions.

However, we prove Conjecture 1 in case K is a finitely-generated extension of $\mathbb{Q}$. In fact we prove the following more general result:

Theorem 1. Let K be a finitely generated extension of $\mathbb{Q}$, let C and D be smooth, projective, geometrically irreducible curves over K, and let $f \colon C \to C$ and $u \colon D \to C$ be morphisms with $\deg(f) > 1$. Then for any $P \in C(K)$, the set $\{n \in \mathbb{N} \colon f^n(P) \in u(D(K))\}$ is the union of finitely many one-sided arithmetic progressions.

This result may be viewed as an arithmetic dynamical analogue of (the cyclic subgroup case of) the Mordell–Lang conjecture, or alternately as an arithmetic analogue of the dynamical Mordell-Lang conjecture. One version of the Mordell–Lang conjecture asserts that if V is any closed subvariety of a complex abelian variety A, and G is a finitely generated subgroup of $A(\mathbb{C})$, then $G \cap V(\mathbb{C})$ is the union of finitely many cosets of subgroups of G. This conjecture was proven by Faltings [7], following earlier work of Vojta [11]. To see the analogy with Theorem 1, consider the case that $G = \langle P \rangle$ is cyclic, and let $f\colon A \to A$ be the map defined by $f(Q) = Q + P$. Then the Mordell–Lang conjecture asserts that $\{n \in \mathbb{Z}\colon f^n(0) \in V(\mathbb{C})\}$ consists of the union of finitely many arithmetic progressions. Theorem 1 may be viewed as an arithmetic analogue of this result, where instead of requiring $f^n(0) \in V(\mathbb{C})$ we instead require $f^n(0) \in u(D(K))$. This perspective suggests generalizing Theorem 1 to the setting of finite morphisms between varieties; we do not know what to expect in this greater generality. Likewise, the "cyclic subgroup case" of the Mordell–Lang conjecture has been generalized conjecturally by Ghioca and Tucker to obtain the dynamical Mordell–Lang conjecture, which asserts that for any endomorphism $f\colon A \to A$ of a complex variety A such that $\deg(f) > 1$, and any subvariety V of $A(\mathbb{C})$, if $P \in A(\mathbb{C})$ then $\{n \in \mathbb{N}\colon f^n(P) \in V(\mathbb{C})\}$ is the union of finitely many one-sided arithmetic progressions. This conjecture has been proven in several special cases [1, 2, 3, 4, 8, 9, 10, 12], but remains open in general. Theorem 1 is an analogue of this conjecture in which the set $V(\mathbb{C})$ is replaced by $u(D(K))$.

One easy case of Theorem 1 is when P is preperiodic under f: for, if $f^i(P) = f^{i+r}(P)$ for some $i, r > 0$, then $f^{j+kr}(P) = f^j(P)$ for every $j \geq i$ and $k \in \mathbb{N}$, whence $\{n \geq i\colon f^n(P) \in u(D(K))\}$ is the union of finitely many one-sided arithmetic progressions with common difference r. Our proof of Theorem 1 shows that there is always some preperiodic behavior in the picture, although in general it is not the sequence of values $f^n(P)$ which is preperiodic, but instead a quite different sequence of objects. Specifically, by considering components of the fibered product of u with f^n for each n, and in particular by considering the degrees of the projections onto C from each such component, we can reduce Theorem 1 to the case that for every n the fibered product of u with f^n is irreducible and has infinitely many K-rational points. This immediately implies that each fibered product is geometrically irreducible, and hence (by Faltings' theorem [6]) has genus at most one. Now the desired preperiodicity occurs in the following result.

Theorem 2. Let K be any field of characteristic zero, let C and D be smooth, projective, geometrically irreducible curves over K, and let $f\colon C \to C$ and $u\colon D \to C$ be morphisms of degree at least 2. Suppose further that for each $n \in \mathbb{N}$ the fibered product E_n of u with f^n is geometrically irreducible of genus at most 1. Let $u_n\colon E_n \to C$ and $w_n\colon E_n \to D$ be the projection maps from this fibered product, so that $f^n \circ u_n = u \circ w_n$. Then the sequence of maps $u_1, u_2, \ldots$ is preperiodic up to isomorphism over K between the domains of the u_n's: that is, there exist positive integers i, r such that for every $s \in \mathbb{N}$ there is an isomorphism $\sigma_s\colon E_{i+rs} \to E_i$ which satisfies $u_{i+rs} = u_i \circ \sigma_s$.

It is not hard to deduce Theorem 1 from Theorem 2. Moreover, we can go a long ways towards classifying all f, u satisfying the hypotheses of Theorem 2: for instance, it turns out that the Galois closure of u must have genus at most 1, and for each such u we can describe the possibilities for the ramification of f.

Here are some follow-up questions:

(1) Can the conclusion of Theorem 1 be refined to only use arithmetic progressions whose common difference is bounded by some function of $\deg(u)$? Likewise, can the common differences be bounded in terms of some data from K? We can show that there cannot be a bound on the common diferences which is independent of both K and u.

(2) If the set described in Theorem 1 is infinite, then is there some integer N which depends only on $\deg(u)$ such that our reduction to the irreducible case takes at most N steps? Explicitly, in case $u, f \in K(X)$ this means that for every irreducible factor $H(X, Y)$ of the numerator of $u(Y) - f^N(X)$ which remains irreducible in $\overline{K}[X, Y]$ and for which (the normalization of) the curve $H(X, Y) = 0$ has genus at most 1, it holds for every $n > 0$ that the numerator of $H(f^n(X), Y)$ defines an irreducible curve over $\overline{K}$ having genus at most 1. A special case of this question is as follows: if $u, f \in K(X)$ satisfy $u \circ v = f^n$ for some $n > 0$ and some $v \in K(X)$, then must there exist $w \in K(X)$ for which $u \circ w = f^N$, where N is a positive integer depending only on $\deg(u)$?

(3) What are the situations in which our reduction to the irreducible case produces more than one tower of fibered products of genus at most 1? For instance, this occurs when $u = f = X^2$, in which case $u(Y) - f^n(X) = (Y - X^{2^{n-1}})(Y + X^{2^{n-1}})$. Are there examples that are significantly more complicated than this?

Finally, it would be interesting to explore higher-dimensional analogues of Theorem 1, or analogues involving the orbit of P under a finitely-generated semigroup of endomorphisms of C.

References

[1] J. P. Bell, *A generalised Skolem–Mahler–Lech theorem for affine varieties*, J. London Math. Soc. (2) **73** (2006), 367–379 (corr. **78** (2008), 267–272).

[2] J. P. Bell, D. Ghioca and T. J. Tucker, *The dynamical Mordell-Lang problem for étale maps*, Amer. J. Math. **132** (2010), 1655–1675.

[3] J. P. Bell, D. Ghioca and T. J. Tucker, *The Dynamical Mordell–Lang Conjecture*, Math. Surveys and Monographs, 210, Amer. Math. Soc., Providence, 2016.

[4] R. L. Benedetto, D. Ghioca, P. Kurlberg and T. J. Tucker, *A case of the dynamical Mordell–Lang conjecture*, Math. Ann. **352** (2012), 1–26.

[5] J. Cahn, R. Jones and J. Spear, *Powers in orbits of rational functions: cases of an arithmetic dynamical Mordell-Lang conjecture*, arXiv:1512.03085v1, December 2015.

[6] G. Faltings, Complements to Mordell, Rational Points (Bonn, 1983/1984), Aspects Math., E6, Vieweg, Braunschweig, 1984, 203–227.

[7] G. Faltings, *The general case of S. Lang's conjecture*, Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), Perspect. Math., 15, Academic Press, San Diego, 1994, 175–182.

[8] D. Ghioca and T. J. Tucker, *Periodic points, linearizing maps, and the dynamical Mordell–Lang problem*, J. Number Theory **129** (2009), 1392–1403.
[9] D. Ghioca, T. J. Tucker and M. E. Zieve, *Intersections of polynomial orbits, and a dynamical Mordell–Lang conjecture*, Invent. Math. **171** (2008), 463–483.
[10] D. Ghioca, T. J. Tucker and M. E. Zieve, *Linear relations between polynomial orbits*, Duke Math. J. **161** (2012), 1379–1410.
[11] P. Vojta, *Siegel's theorem in the compact case*, Ann. of Math. (2) **133** (1991), 509–548.
[12] J. Xie, *Dynamical Mordell–Lang conjecture for birational polynomial morphisms on* $\mathbb{A}^2$, Math. Ann. **360** (2014), 457–480.

Heights and preperiodic points for certain polynomials

Patrick Ingram

Let K be a number field, and let $f(z) \in K(z)$ be a rational function of degree $d \geq 2$. Then it is a consequence of basic properties of the Weil height that the set

$$\mathrm{Preper}(f, K) = \{z \in \mathbb{P}^1(K) : f^n(z) = f^m(z) \text{ for some } n \neq m\}$$

is finite. On the other hand, one can show just using linear algebra that

$$\sup_{\substack{f(z)\in K(z)\\ \deg(f)=d}} \#\,\mathrm{Preper}(f, K) \geq d + 1.$$

It is natural to ask, then, whether or not there is a uniform bound on $\#\,\mathrm{Preper}(f, K)$ once $\deg(f)$ and K are fixed (or perhaps $\deg(f)$ and $[K : \mathbb{Q}]$).

Conjecture 1 (Morton-Silverman [5])**.** There is a bound on $\#\,\mathrm{Preper}(f, K)$ which depends just on $\deg(f)$ and K.

A more modest question is, "Can we exhibit a single family of rational functions for which we can prove Conjecture 1?" Without any caveats, the answer to this question is an easy yes. If the family is constant, or more generally isotrivial, then it is easy to obtain a uniform bound.

Less obviously, one can also prove a uniform bound for so-called Lattès examples. For instance, suppose that $f(z) \in K(z)$ fits into a commutative diagram of the form

$$\begin{array}{ccc} E & \xrightarrow{[m]} & E \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ \mathbb{P}^1 & \xrightarrow[f]{} & \mathbb{P}^1 \end{array}$$

for E/K an elliptic curve, and π non-constant. From the diagram, K-rational preperiodic points for f pull back to L-rational torsion points on E for some L/K with $[L : K] \leq \deg(\pi)$. Merel's Theorem [4] then gives us a uniform bound on the number of such points, depending on m and K (actually $[K : \mathbb{Q}]$), but not on E or f. Lattès examples are perhaps not a satisfactory answer to the question, though. In complex dynamics these functions turn out to be the exceptional case to many theorems, and so the fact that the conjecture holds here is not particularly reassuring.

Associated to a rational function f is a *canonical height* $\hat{h}_f$, defined by

$$\hat{h}_f(z) = \lim_{n\to\infty} d^{-n} h \circ f^n(z).$$

This function vanishes precisely on preperiodic points, and it is natural to make the following conjecture (essentially a conjecture of Silverman [6, Conjecture 4.98, p. 221] building on one of Lang).

Conjecture 2. Let K be a number field, and fix a non-isotrivial family f_t of rational functions of generic degree $d \geq 2$ parametrized over the curve U. There exist $\varepsilon > 0$ and $N \geq 0$ such that for all $t \in U(K)$

$$\hat{h}_{f_t}(z) \geq \varepsilon h(t)$$

for all but at most N values $z \in \mathbb{P}^1(K)$.

We consider the problem for *weighted homogeneous* families $f_t(z)$ of polynomials, that is, families such that there exists a binary homogeneous form $F(x, y)$, not divisible by x or y, and an integer $e \geq 2$ such that $f_t(z) = F(z^e, t)$. The archetype is the family $f_t(z) = z^d + t$ of unicritical polynomials of degree $d = e \geq 2$. We can prove a weak form of Conjecture 2 for families of this form.

Theorem 1 (Ingram [2], Ingram [3])**.** Let K be a number field, and fix a weighted homogeneous family f_t of rational functions of generic degree $d \geq 2$ parametrized over the curve U. For any s there exist $\varepsilon > 0$ and $N \geq 0$ such that for all $t \in U(K)$ integral away from at most s places

$$\hat{h}_{f_t}(z) \geq \varepsilon h(t)$$

for all but at most N values $z \in \mathbb{P}^1(K)$.

Implicit in this is a weak form of Conjecture 1 for weighted homogeneous families, but depending on the number of places of bad reduction. This consequence, however, is vastly superseded by Benedetto's Theorem [1] bounding the number of preperiodic points of a polynomial in terms of the number of places of bad reduction (see also [5] for a result for rational functions).

If we are willing to give ourselves more freedom in constructing examples, however, we can do better. Consider the family obtained by extending the base by $t = \varphi(u)$. If $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ is sufficiently general, we can remove the dependence on the number of bad primes.

Theorem 2 (Ingram [3])**.** Let K be a number field, and fix a weighted homogeneous family $f_t(z) = F(z^e, t)$ of rational functions of generic degree $d \geq 2$ parametrized over the curve U. Suppose further that $\varphi(u) \in K(u)$ has at least N_e affine poles of order prime to e, where

$$N_e = \begin{cases} 5 & e = 2 \\ 4 & e = 3 \\ 3 & e \geq 4. \end{cases}$$

(1) There is a uniform bound on $\#\operatorname{Preper}(f_{\varphi(u)}, K)$, for K-rational u.

(2) Assuming the *abc* Conjecture for K, there exist constants $\varepsilon > 0$ and N (depending in K, f, and φ, but not u) such that

$$\hat{h}_{f_{\varphi(u)}}(z) \geq \epsilon h(u)$$

for all but N values $z \in \mathbb{P}^1$.

References

[1] R. Benedetto. *Preperiodic points of polynomials over global fields*. J. Reine Ange. Math. **608** (2007), 123–153.

[2] P. Ingram, *Lower bounds on the canonical height associated to the morphism* $\phi(z) = z^d + c$, Monat. Math. **157** (2009), 69–89.

[3] P. Ingram. *Canonical heights and preperiodic points for weighted homogeneous families of polynomials*, arXiv:1510.08807.

[4] L. Merel. *Borne pour la torsion des courbes elliptiques sur les corps de nombres*. Invent. Math. **124** (1996), 437–449.

[5] P. Morton and J. H. Silverman. *Rational Periodic Points of Rational Functions*. Int. Math. Res. Not. **2** (1994), 97–110.

[6] J. H. Silverman. *The Arithmetic of Dynamical Systems*, volume 241 of *Graduate Texts in Mathematics*. Springer, 2007.

Diversity in Parametric Families of Number Fields

Yuri Bilu

(joint work with Florian Luca)

Let X be an algebraic curve over $\mathbb{Q}$ of genus $\mathbf{g}$ and $t \in \mathbb{Q}(X)$ a non-constant rational function of degree $\nu \geq 2$. We fix, once and for all, an algebraic closure $\bar{\mathbb{Q}}$. For every positive integer n pick $P_n \in X(\bar{\mathbb{Q}})$ such that $t(P_n) = n$.

According to the classical Hilbert's Irreducibility Theorem, for infinitely many n we have $[\mathbb{Q}(P_n) : \mathbb{Q}] = \nu$. Hilbert's Irreducibility Theorem, however, does not answer the following natural question: among the field $\mathbb{Q}(P_n)$, are there "many" distinct (in the fixed algebraic closure $\bar{\mathbb{Q}}$)? This question is addressed in the article of Dvornicich and Zannier [2], where the following theorem is proved (see [2, Theorem 2(a)]).

Theorem 1 (Dvornicich, Zannier)**.** In the above set-up, there exists a positive real number $c = c(\mathbf{g}, \nu)$ such that for sufficiently large integer N we have

$$[\mathbb{Q}(P_1, \dots, P_N) : \mathbb{Q}] \geq e^{cN/\log N}.$$

An immediate consequence is the following result.

Corollary 1. In the above set-up, there exists a real number $c = c(\mathbf{g}, \nu) > 0$ such that for every sufficiently large integer N, among the number fields

$$\mathbb{Q}(P_1), \dots, \mathbb{Q}(P_N) \tag{1}$$

there are at least $cN/\log N$ distinct.

Theorem 1 is best possible, as obvious examples show. Say, if X is the plane curve $t = u^2$ and t is the coordinate function, then

$$\mathbb{Q}(P_1, \dots, P_N) = \mathbb{Q}(\sqrt{1}, \sqrt{2}, \dots, \sqrt{N}) = \mathbb{Q}(\sqrt{p} : p \le N)$$

is of degree $2^{\pi(N)} \le e^{cN/\log N}$.

On the contrary, Corollary 1 does not seem to be best possible. For instance, in the same example, if n runs the square-free numbers among $1, \dots, N$ then the fields $Q(P_n) = \mathbb{Q}(\sqrt{n})$ are pairwise distinct. It is well-known that among $1, \dots, N$ there is, asymptotically, $\zeta(2)^{-1}N$ square-free numbers as $N \to \infty$.

We suggest the following conjecture.

Conjecture 1 (Weak Diversity Conjecture)**.** In the above set-up there exists a real number $c = c(\mathbf{g}, \nu) > 0$ such that for every sufficiently large integer N, among the number fields (1) there are at least cN distinct.

Conjecture 1 relates to Corollary 1 in the same way as the following conjecture (attributed in [2] to Schinzel) relates to Theorem 1.

Conjecture 2 (Strong Diversity Conjecture (Schinzel))**.** Assume that either t has at least one finite critical value not belonging to $\mathbb{Q}$, or the field extension $\bar{\mathbb{Q}}(X)/\bar{\mathbb{Q}}(t)$ is not abelian. Then there exists a real number $c = c(\mathbf{g}, \nu) > 0$ such that for every sufficiently large integer N we have

$$[\mathbb{Q}(P_1, \dots, P_N) : \mathbb{Q}] \ge e^{cN}.$$

(We call $\alpha \in \bar{\mathbb{Q}} \cup \{\infty\}$ a *critical value* of t if the rational function $t - \alpha$ has at least one multiple zero in $X(\bar{\mathbb{Q}})$, with the standard convention $t - \infty = 1/t$.)

As Dvornichich and Zannier remark, the hypothesis in the Strong Diversity Conjecture conjecture is necessary. Indeed, when all critical values belong to $\mathbb{Q}$ and the field extension $\bar{\mathbb{Q}}(X)/\bar{\mathbb{Q}}(t)$ is abelian, it follows from Kummer's Theory that $\mathbb{Q}(X)$ is contained in the field of the form $L(t, (t-\alpha_1)^{1/e_1}, \dots, (t-\alpha_s)^{1/e_s})$, where L is a number field, $\alpha_1, \dots, \alpha_s$ are rational numbers and $e_1, \dots, e_s$ are positive integers. Clearly, in this case the degree of the number field generated by $P_1, \dots, P_N$ cannot exceed $e^{cN/\log N}$ for some $c > 0$.

It is easy to see that Conjecture 2 implies Conjecture 1.

Dvornicich and Zannier obtain several results in favor of Conjecture 2. In particular, they show [2, Theorem 2(b)] that it holds true if t admits a critical value of degree 2 or 3 over $\mathbb{Q}$.

Our principal result [1] is a little progress in the direction of Conjecture 1.

Theorem 2 (Yu. Bilu, F. Luca)**.** We keep the above set-up. There exists a real number $\eta = \eta(\mathbf{g}, \nu) > 0$ such that for every sufficiently large integer N, among the number fields (1) there are at least $N/(\log N)^{1-\eta}$ distinct.

The proof uses a modification of the ramification argument of Dvornicich and Zannier, with prime numbers replaced by suitably chosen square-free numbers.

References

[1] Yu. F. Bilu, F. Luca, Diversity in Parametric Families of Number Fields, a manuscript.
[2] R. Dvornicich, U. Zannier, Fields containing values of algebraic functions, *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **21** (1994), 421–443.

The Bounded Height Conjecture for semiabelian varieties

Lars Kühne

In (all of) the sequel, G is a semiabelian variety endowed with a G-linearized ample line bundle $\mathcal{L}$ and X is a closed subvariety of G. In addition, assume that G, $\mathcal{L}$, and X are defined over $\overline{\mathbb{Q}}$. We denote the abelian variety underlying G by A and its maximal subtorus by T. Finally, let $h_{\mathcal{L}} : G(\overline{\mathbb{Q}}) \to \mathbb{R}$ be a Weil height associated with $\mathcal{L}$.

Since the pioneering work of Bombieri, Masser, and Zannier [2], intersections of X with algebraic subgroups of G have been widely studied in diophantine geometry. Of course, investigating the intersection of X with a single such subgroup is a dreary task. However, very interesting phenomena appear when intersecting $X \subseteq G$ with the countable union $G^{[s]}$ of *all* algebraic subgroups having codimension $\geq s$ for some fixed integer s. In fact, taking $s = \dim(X) + 1$ leads to so-called unlikely intersection problems, on which a comprehensive overview can be found in [10]. Basically, conjectures of Pink [7] and Zilber [11] state that $X \cap G^{[\dim(X)+1]}$ should be finite for sufficiently generic X.

In my recent work [6], I consider the other important and related case where $s = \dim(X)$. In this case, a generic subgroup $H \subset G$ of codimension $\geq s$ intersects X already in finitely many points so that $X \cap G^{[\dim(X)]}$ is definitely not finite. The gist of the Bounded Height Conjecture (BHC) stated below is that the Weil height of the $\overline{\mathbb{Q}}$-points in $X \cap G^{[\dim(X)]}$ should be nevertheless bounded from above.

In order to state this conjecture concisely, one has to introduce some additional notions to tackle also non-generic cases. In fact, one defines X^{oa} as X deprived by its "anomalous" intersections with algebraic subgroups of G; a precise definition can be found in [5]. One can actually show that X^{oa} is a Zariski open (but possibly empty) subset of X. For tori this fact is due to Bombieri, Masser, and Zannier [3] and for abelian varieties it was proven by Rémond [8]. The extension to semiabelian varieties is straightforward. We can now state the

Conjecture 1. (Bounded Height Conjecture, BHC). The height $h_{\mathcal{L}}$ is bounded from above on the intersection $X^{\mathrm{oa}}(\overline{\mathbb{Q}}) \cap G^{[\dim(X)]}(\overline{\mathbb{Q}})$.

This conjecture was first proposed by Bombieri, Masser, and Zannier [3] in the case where G is a torus. Even before this, they had provided a proof [2] if G is a torus and X is a curve. The extension of their conjecture from tori to semiabelian varieties is merely formal and can be found in Habegger's article [4], where also a proof of the BHC for abelian varieties is given. In parallel to his work on the BHC for abelian varieties, Habegger [5] obtained a complete proof of the conjecture for tori. Regarding the general case of the BHC, no further progress has been

made since Habegger's breakthrough articles [4, 5]. In fact, the "mixed" nature of semiabelian varieties induces completely new problems so that all attempts failed until recently.

Theorem 1 (K. 2016)**.** The BHC is true in general.

The overall strategy is not too much different from that used by Habegger in [4, 5]. Since I could not give a complete sketch of the argument in the thirty minutes of my conference talk and there is a strict page limit on this report, I dwell here on the first part of the proof as I did in Oberwolfach. In addition, I believe this part to be of most interest for other research related to semiabelian varieties.

Sketch of the proof. Instead of working with subgroups $H \subset G$, $\operatorname{codim}(H) \geq \dim(X)$, we use the corresponding quotients $G \to G/H$, $\dim(G/H) \geq \dim(X)$. We aim to approximate these countably many quotients (and thereby their kernels H) by a *finite* number of surjective quasi-homomorphisms $\varphi_i \in \operatorname{Hom}_{\mathbb{Q}}(G, G_0) = \operatorname{Hom}(G, G_0) \otimes_{\mathbb{Z}} \mathbb{Q}$. The corresponding step in [4, 5] is rather inconspicuous but for semiabelian varieties a substantial problem occurs: In fact, let $\mathcal{S}_G$ be the set of all isogeny classes $[H]$ of semiabelian varieties H for which there is a surjective homomorphism $G \to H$. Clearly, $\mathcal{S}_G$ is finite if G is a torus or an abelian variety (by Poincare reducibility) but not in general. Nevertheless, fixing representatives B_l, $1 \leq l \leq m$, of $\mathcal{S}_A$ one can find in each isogeny class contained in $\mathcal{S}_G$ a semiabelian variety whose underlying abelian variety is some B_{l_0}, $1 \leq l_0 \leq m$. We restrict to such quotients $G \to G_0$ in the following. Furthermore, any quasi-homomorphism $\varphi \in \operatorname{Hom}_{\mathbb{Q}}(G_1, G_2)$ between two semiabelian varieties can be described in terms of the induced quasi-homomorphism $\varphi_t \in \operatorname{Hom}_{\mathbb{Q}}(T_1, T_2)$ of the maximal tori and the induced quasi-homomorphism $\varphi_a \in \operatorname{Hom}_{\mathbb{Q}}(A_1, A_2)$ of the underlying abelian varieties. In fact, the pairs (φ_t, φ_a) that are associated to a homomorphism $G_1 \to G_2$ are described by $(\varphi_t)_* \eta_{G_1} = (\varphi_a)^* \eta_{G_2}$ where $\eta_{G_i} \in \operatorname{Ext}^1(A_i, T_i)$ is the extension class associated with G_i (see [9, Chapter VII]).[1] Therefore, we may try to approximate (φ_t, φ_a) (instead of $\varphi : G \to G_0$) within the $\mathbb{Q}$-vector spaces

$$V_{kl} = \operatorname{Hom}_{\mathbb{Q}}(T, \mathbb{G}_m^k) \times \operatorname{Hom}_{\mathbb{Q}}(A, B_l),\ 0 \leq k \leq \dim(T),\ 1 \leq l \leq m.$$

Of course, we mean here to approximate (φ_t, φ_a) with pairs (φ_t', φ_a') associated with other quasi-homomorphisms $\varphi' : G \to G_0'$. At first sight, the subset $Z \subseteq V_{kl}$ of such pairs (φ_t', φ_a') seems to form a linear $\mathbb{Q}$-subspace of V_{kl} because of the 'linear relation' $(\varphi_t')_* \eta_G = (\varphi_a')^* \eta_{G_0'}$. *This is completely wrong because $\eta_{G_0'}$ is not fixed (in particular, we may have $G_0 \neq G_0'$) but varies along with (φ_t', φ_a').* Hence, we do not know much on Z and our intermediate lemmas are substantially weaker but easier to prove than those in [4, 5] as we have not much knowledge about Z. (Actually, Z is the set of $\mathbb{Q}$-rational points of an algebraic subvariety in the affine space V_{kl}. However, easy examples show that one should not expect much helpful information from this.) We have to account for this weakness at other places.

[1] The equality $(\varphi_t)_* \eta_{G_1} = (\varphi_a)^* \eta_{G_2}$ makes formally only sense for homomorphisms. However, it is also true for quasi-homomorphisms if interpreted properly.

Lemma 1. There exist some compact subsets $\mathcal{K}_{kl} \subset V_{kl}$ such that for any point $p \in G^{[\dim(X)]}(\overline{\mathbb{Q}})$ there exists some surjective quasi-homomorphism $\varphi \in \mathrm{Hom}_{\mathbb{Q}}(G, G_0)$, $\dim(G_0) \geq \dim(X)$, with $(\varphi_t, \varphi_a) \in \mathcal{K}_{kl}$ (for some k, l) and $p \in \ker(\varphi) + \mathrm{Tor}(G)$.

Note that both the notion of surjectivity and $\ker(\varphi) + \mathrm{Tor}(G)$ make sense for a quasi-homomorphism φ.

Lemma 2. For any $\delta > 0$, there exist finitely many surjective quasi-homomorphisms $\varphi_i \in \mathrm{Hom}_{\mathbb{Q}}(G, G_i)$, $1 \leq i \leq n(\delta)$, such that any surjective quasi-homomorphism $\varphi \in \mathrm{Hom}_{\mathbb{Q}}(G, G_0)$ with $(\varphi_t, \varphi_a) \in \mathcal{K}_{kl}$ satisfies

$$\max\{|\varphi_{i_0,a} - \varphi_a|, |\varphi_{i_0,t} - \varphi_t|\} < \delta$$

for some $1 \leq i_0 \leq n(\delta)$.

This lemma is straightforwardly proven by the pigeonhole principle.

The remainder of the proof establishes two competing height bounds in the situations prepared by the above lemmas. For δ sufficiently small, these yield the boundedness of $h_{\mathcal{L}}$ on $X^{\mathrm{oa}}(\overline{\mathbb{Q}}) \cap G^{[\dim(X)]}(\overline{\mathbb{Q}})$. A further problem to be resolved is that the canonical height on a semiabelian variety cannot be chosen to be homogeneous as for an abelian variety. However, some clever choice of line bundles remedies this.

In addition, we need some bounds on intersections numbers to apply a corollary to a result of Siu on big line bundles. This resembles the proof in [4, 5]. However, the needed bounds on intersection numbers are obtained by using explicit Chern forms. This allows for an effective proof in the cases where one does not need the pigeonhole principle in Lemma 2 because one has more information on Z. In this way, the proof gives an effective version of the BHC for abelian varieties – in contrast to the proof of [4].

□

References

[1] D. Bertrand, *Endomorphismes de groupes algébriques; applications arithmétiques* in: *Diophantine approximations and transcendental numbers (Luminy, 1982)*, Birkhäuser 1983, 1–45.

[2] E. Bombieri, D. Masser, and U. Zannier, *Intersecting a curve with algebraic subgroups of multiplicative groups*, IMRN **1999 (20)**, 1119–1140.

[3] E. Bombieri, D. Masser, and U. Zannier, *Anomalous subvarieties – structure theorems and applications*, IMRN **2007 (19)**, 1–33.

[4] P. Habegger, *Intersecting subvarieties of abelian varieties with algebraic subgroups of complementary dimension*, Invent. Math. **176** (2009), 405–447.

[5] P. Habegger, *On the bounded height conjecture*, IMRN **2009 (5)**, 860–886.

[6] L. Kühne, *The Bounded Height Conjecture for semiabelian varieties*, in preparation.

[7] R. Pink, *A common generalization of the conjectures of André-Oort, Manin-Mumford, and Mordell-Lang*, available from `http://www.math.ethz.ch/~pink`, April 2005.

[8] G. Rémond, *Intersection de sous-groupes et de sous-variétés III*, Comment. Math. Helv. **84** (2009), 835–863.

[9] J.-P. Serre, *Algebraic groups and class fields*, Graduate Texts in Mathematics **117**, Springer 1988.

[10] U. Zannier, *Some problems of unlikely intersections in arithmetic and geometry*, Annals of Mathematics Studies **181**, Princeton University Press, 2012.
[11] B. Zilber, *Exponential sums equations and the Schanuel conjecture*, J. London Math. Soc. (2) **65** (2002), 27–44.

Brauer-Siegel estimates for abelian varieties

Marc Hindry
(joint work with Amílcar Pacheco)

We discuss analogues of the classical Brauer-Siegel theorem for abelian varieties over global fields. A global field K is either a number field or the function field of a curve over a finite field $K = \mathbf{F}_q(C)$. We speak accordingly of the *number field* case (nf), or the *function field* case (ff).

The classical Brauer-Siegel theorem states that, for number fields F of fixed (or bounded) degree, the product of the class number h_F by the regulator of units R_F behaves asymptotically like the square root of the absolute value of the discriminant Δ_F. In symbols we may write, when $\Delta_F \to \infty$:

$$\frac{\log(h_F R_F)}{\log\sqrt{\Delta_F}} \sim 1 \quad \text{or} \quad C_\epsilon^{-1}\Delta^{\frac{1}{2}-\epsilon} \leq h_F R_F \leq C_\epsilon \Delta^{\frac{1}{2}+\epsilon}$$

When A is an abelian variety of dimensionn g defined over a global field K, we consider g and K fixed, and A varying, by insisting that the *exponential height* $H(A) = H(A/K)$ goes to infinity. The analogue we have in mind is the question

$$\frac{\log(|Ш(A/K)|\mathrm{Reg}(A/K))}{\log H(A/K)} \sim 1?$$

or

$$C_\epsilon^{-1} H(A/K)^{1-\epsilon} \leq |Ш(A/K)|\,\mathrm{Reg}(A/K) \leq C_\epsilon H(A/K)^{1+\epsilon}?$$

Here $Ш(A/K)$ denotes the Shafarevich-Tate group which may be quickly defined as

$$Ш(A/K) = \mathrm{Ker}\left\{ H^1(G_K, A) \to \prod_v H^1(G_{K_v}, A_{K_v}) \right\}$$

where we denote K^s the separable closure of K and G_K the Galois group of K^s/K. Also $\check{A}$ denotes the dual abelian variety and the Néron-Tate *regulator* is defined as $\mathrm{Reg}(A/K) := \det\langle P_i, \check{P}_j\rangle$, where $\langle\cdot,\cdot\rangle$ is the canonical "Poincaré-Néron-Tate" height pairing on $A(K) \times \check{A}(K)$ and $P_1, \ldots, P_r$ (resp. $\check{P}_1, \ldots, \check{P}_r$) is a basis of $A(K)$ (resp. $\check{A}(K)$) modulo torsion.

We briefly comment that that the regulator $\mathrm{Reg}(A/K)$ is a good measure of the complexity of a basis of the Mordell-Weil group $A(K)$, since it controls the size of (minimal) generators of the group, whereas the cardinality of the Shafarevich-Tate group is a good measure of the size of the obstructions to computing the Mordell-Weil group via descent. Thus the fact that the product of the cardinality of the Shafarevich-Tate group by the regulator seems to be often very large (exponential

in the data $h(A/K) = \log H(A/K)$) tends to indicate that computing the Mordell-Weil group is a hard problem.

Such statement implicitly assume finiteness of the Shafarevich-Tate group. The analogy has two sources, first the class group of a number field can be seen as a Shafarevich-Tate group for the group of units, second there is a formal analogy between the class number formula and the Birch & Swinnerton-Dyer conjectural formula

$$\lim_{s\to 1}(s-1)\zeta_F(s) = \frac{h_F R_F}{\sqrt{\Delta_F}} \frac{2^{r_1}(2\pi)^{r_2}}{|\mu_F|}$$

and

$$\lim_{s\to 1}(s-1)^{-r} L(A/K,s) \stackrel{?}{=} \frac{|Ш(A/K)|\operatorname{Reg}(A/K)}{\tilde{H}(A/K)} \frac{\prod_v c_v(A/K)}{|(A\times \check{A}(K)_{\mathrm{tor}}|}.$$

Here $\tilde{H}(A/K) = H(A/K)$ in the function field case (ff) but $\tilde{H}(A/K)$ is the inverse of the period of A/K in the number field case (nf). However it can be shown (see [2]) that $H(A/K) \ll \tilde{H}(A/K) \ll H(A/K)^{1+\epsilon}$. The factor $\prod_v c_v(A/K)$ is sometimes called the Tamagawa number, it is equal to the product over all places (with bad reduction) of the indices $(A(K_v) : A^0(K_v))$ where $A^0(K_v)$ is the subgroup of points extending to the neutral component of the Néron model of A.

The Birch & Swinnerton-Dyer is of course conjectural in general, however, in the function field case the situation is far better: the full conjecture is known to be a consequence of the finiteness of one ℓ-primary component of the Shafarevich-Tate goup (this is due to a series of paper starting with Tate, Milne, ..., and culminating with [4]).

Theorem 1. [2, 3] Assume finiteness of the Shafarevich-Tate goup, in the number field case assume analytical continuation of the L-function $L(A/K, s)$ satifying the natural functional equation and generalised Riemann hypothesis. We have

$$|Ш(A/K)|\operatorname{Reg}(A/K) \leq C_\epsilon H(A/K)^{1+\epsilon}$$

Noting that $|Ш(A/K)|$ is an integer and using the diophantine estimate $\operatorname{Reg}(A/K) \geq C'_\epsilon H(A/K)^{-\epsilon}$, we get as a corollary that, under the same conditions, both $|Ш(A/K)|$ and $\operatorname{Reg}(A/K)$ are $O\left(H(A/K)^{1+\epsilon}\right)$.

There remains the question of wether the estimate from the theorem is best possible or, in other words, wether the classical Brauer-Siegel estimate holds. Unfortunately we leave this question unanswered but provide the following clues.

To express the problem we introduce the *Brauer-Siegel ratio* as

$$\mathrm{BS}\,(A/K) := \frac{\log\{|Ш(A/K)|\operatorname{Reg}(A/K)\}}{\log H(A/K)}$$

By estimating the term $H(A/K)^{-\epsilon} \ll \frac{\prod_v c_v(A/K)}{|(A\times \check{A}(K)_{\mathrm{tor}}|} \ll H(A/K)^{\epsilon}$ (the estimate is relatively easy for elliptic curves but delicate for higher dimension abelian varieties, see [2, 3]) and combining with the previous results we get:

$$0 \leq \liminf_{H(A/K)\to\infty} \mathrm{BS}\,(A/K) \leq \limsup_{H(A/K)\to\infty} \mathrm{BS}\,(A/K) = 1.$$

Replacing ≤ 1 by $= 1$, in the previous inequality, requires the following kind of unconditional examples.

Theorem 2. The following estimates are valid for the following explicit families:

(1) (see [3]) Let d be coprime to the characteristic of $K = \mathbf{F}_q(t)$ and (E_d) the elliptic curve defined by $y^2 + y = x^3 + t^d$.
(2) (Griffon, see [1]) Let d be coprime to the characteristic of $K = \mathbf{F}_q(t)$ and (E_d) the "Legendre" elliptic curve defined by $y^2 = x(x+1)(x+t^d)$.

The Shafarevich-Tate group of E_d/K is finite (unconditionally) and

$$\lim_{d\to\infty} \mathrm{BS}\,(E_d/K) = 1.$$

Richard Griffon's thesis contains many more examples of families with a similar behaviour. However other situations suggest that the classical Brauer-Siegel theorem is not true in general and the "lim inf" of the Brauer-Siegel ratio should be zero.

One such situation is the case of *twists* of a given elliptic curve, i.e. a curve E_D with equation $Dy^2 = x^3 + ax + b$, with D either a squarefree integer – case (nf) with $K = \mathbf{Q}$ – or a squarefree polynomial in $\mathbf{F}_q[t]$ – case (ff) with $K = \mathbf{F}_q(t)$. There a theorem of Waldspurger (extended to the function field setting by Altuğ–Tsimerman) states essentially that:

$$L(E_D, 1) = \kappa \frac{c(|D|)^2}{\sqrt{|D|}}$$

where $c(|D)|)$ is the Fourier coefficient of the weight $3/2$ modular form associated to E by Shimura theory and modularity of E. The estimates translate in this context as

$$0 \leq \liminf \frac{\log|c(|D|)|}{\log|D|} \leq \limsup \frac{\log|c(|D|)|}{\log|D|} = \frac{1}{4}.$$

The estimate for the limit sup is a theorem in the function field case and the Ramanujan conjecture in the number field case. Heuristics suggest a distribution of Fourier coefficient where the limit inf would be zero (see [3] for a discussion and an analysis of the case where E is a constant curve, i.e. defined over $\mathbf{F}_q$).

References

[1] R. Griffon, *Analogues du théorème de Brauer-Siegel pour quelques familles de courbes elliptiques*, Thèse université Paris Diderot Paris 7, 2016.

[2] M. Hindry, *Why is it difficult to compute the Mordell-Weil group?*, *in* Diophantine geometry CRM Series, vol. 4, Ed. Norm., Pisa, 2007, 197–219.

[3] M. Hindry, A. Pacheco, *An analogue of the Brauer-Siegel theorem for abelian varieties in positive characteristic*, Moscow Mathematical Journal**16** (2016), 45–93.

[4] K. Kato and F. Trihan, *On the conjectures of Birch and Swinnerton-Dyer in characteristic* $p > 0$, Invent. Math. **153** (2003), 537–592.

Determinants and irrationality

Wadim Zudilin

It is a classical fact that the irrationality of a number $\xi \in \mathbb{R}$ follows from the existence of a sequence p_n/q_n with integral p_n and q_n such that $q_n\xi - p_n \neq 0$ for all n and $q_n\xi - p_n \to 0$ as $n \to \infty$. A way to formalise this is as follows.

Suppose we have a sequence of rational approximations

$$r_n = a_n\xi - b_n \in \mathbb{Q}\xi + \mathbb{Q}$$

such that

(a) $0 < r_n \le C_1\varepsilon^n$ for some $C_1, \varepsilon > 0$ and all $n = 1, 2, \dots$;
(b) $\delta_n a_n, \delta_n b_n \in \mathbb{Z}$ for some sequence of positive integers δ_n; and
(c) $\delta_n < C_2\Delta^n$ for some $C_2, \Delta > 0$ and all $n = 1, 2, \dots$.

Proposition 1. Under hypotheses (a)–(c), if $\varepsilon\Delta < 1$ then ξ is irrational.

In the talk we explain that under some further (natural) assumptions on the approximants $r_n = a_n\xi - b_n$ we can replace the condition $\varepsilon\Delta < 1$ by a slightly different one. Namely, assume additionally that

(d) $r_n = \displaystyle\int_\gamma z(\boldsymbol{x})^n\omega(\boldsymbol{x})$ for some domain $\gamma \subset \mathbb{R}^m$, non-constant continuous function $z(\boldsymbol{x}) \ge 0$ on γ and measure (positive differential form) $\omega(\boldsymbol{x})$; and
(e) δ_n divides δ_{n+1} for all $n = 1, 2, \dots$.

Proposition 2. Under hypotheses (a)–(e), if $\varepsilon\Delta^{3/2}/4 < 1$ then ξ is irrational.

The proof exploits the Hankel determinants $\det_{0\le j,\ell<n}(r_{j+\ell})$ of the sequence r_n; details can be found in [6]. Note that $\varepsilon\Delta^{3/2}/4 < (\varepsilon\Delta)^{3/2}$ if $\varepsilon > 1/16$, so that Proposition 2 is sometimes conclusive when Proposition 1 is not. For example, the linear approximations

$$\begin{aligned} I_n(a) &= \int_1^a \frac{(x-1)^n(a-x)^n}{x^{n+1}}\,\mathrm{d}x \\ &= \sum_{\substack{j,\ell=0\\ j+\ell\neq n}}^{n} \binom{n}{j}\binom{n}{\ell}(-1)^{n+j+\ell}\,\frac{a^j - a^{n-\ell}}{j+\ell-n} + (\log a)\sum_{j=0}^{n}\binom{n}{j}^2 a^j \end{aligned}$$

to $\log a$, where $n = 0, 1, 2, \dots$, can be used for $a = 3$ and $a = i$ together with Proposition 2 for proving that the numbers $\log 3$ and π are irrational. In fact, the change of variable $x = (1+it)/(1-it)$ transforms $I_n(i)$ into

$$I_n(i) = 2^{n+1}i(-1-i)^n \int_0^1 \frac{t^n(1-t)^n}{(1+t^2)^{n+1}}\,\mathrm{d}t;$$

a normalization of the resulting integral is real, hence legitimate to the use of Proposition 2. The impossibility to use the rational approximations to π originated from the integrals $I_n(i)$ is recorded in the literature [1, 2].

A counterpart of Proposition 2 in the context of the values of q-series is discussed in [7], where the irrationality of

$$\sum_{n=1}^{\infty} \frac{q^n z^n}{1-q^n x}$$

is deduced for q of the form $1/q \in \mathbb{Z} \setminus \{0, \pm 1\}$ and nonzero rational x, z for which the series converges.

The fact that irrationality of numbers can be deduced from polynomial (rather than linear) approximations coming from the Hankel determinants seems to be underexploited; other appearances in a slightly different setting can be found in [3, 5]. A different arithmetic application of the Hankel determinants

$$\det_{0 \le j,\ell < n} \big(\zeta(a(j+\ell)+b)\big)$$

is discussed in [4].

Assuming additionally that

(f) $0 < |a_n| \le C_3 \Lambda^n$ for some $C_3, \Lambda > 0$ and all $n = 1, 2, \dots$,

we can further extend Proposition 2 to a non-algebraicity criterion (see also [5, Section 5] for a similar discussion).

Proposition 3. Under hypotheses (a)–(f), if $\varepsilon \Delta^{3d/2} \Lambda^{d-1}/4 < 1$ then ξ is not an algebraic number of degree $\le d$.

For comparison, Liouville's bound for the same conclusion reads $\varepsilon \Delta^d \Lambda^{d-1} < 1$.

The use of Hankel determinants naturally raises a question about how small the quantity

$$\Big| \det_{0 \le j,\ell < n} \big(q_{j+\ell}\xi - p_{j+\ell}\big) \Big|$$

can be under the constraint $1 \le \max_{0 \le j \le 2n-2} \{|p_j|, |q_j|\} \le D$; namely, an estimate from above for the determinant of the form D^{-v} for some $v = v(n)$. When $n = 1$ Dirichlet's classical theorem answers the question: $v(1) = 1$. The problem looks harder when $n > 1$.

References

[1] K. Alladi and M. L. Robinson, *On certain irrational values of the logarithm*, in "Number theory, Carbondale 1979", Lecture Notes in Math. **751** (Springer, Berlin, 1979), 1–9.

[2] F. Beukers, *A rational approach to* π, Nieuw archief voor wiskunde (5) **1** (2000), no. 4, 372–379.

[3] J.-P. Bézivin, *Sur les propriétés arithmétiques d'une fonction entière*, Math. Nachr. **190** (1998), no. 1, 31–42.

[4] A. Haynes and W. Zudilin, *Hankel determinants of zeta values*, SIGMA **11** (2015), 101, 5 pp.

[5] 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), no. 3, 243–269.

[6] W. Zudilin, *A few remarks on linear forms involving Catalan's constant*, Constr. Approx. (to appear); doi: 10.1007/s00365-016-9333-7.

[7] W. Zudilin, *On the irrationality of generalized q-logarithm*, Res. Number Theory (to appear); arXiv: 1601.02688 [math.NT].

The saddle-point method in $\mathbb{C}^N$

Carlo Viola
(joint work with F. Pinna)

The quest for qualitative or quantitative results of irrationality, of non-quadraticity, ..., or of linear independence over $\mathbb{Q}$ for values of special functions at rational numbers requires to separate values v_h by means of simultaneous rational approximations, i.e., by linear forms $p_{hn} - q_n v_h$ with $p_{hn}, q_n \in \mathbb{Z}$, and to get asymptotic estimates, from above and from below, for $|p_{hn} - q_n v_h| \to 0$ and $|q_n| \to \infty$ as $n \to +\infty$.

In explicit examples, both the construction of linear forms $p_{hn} - q_n v_h$ and the proof of the required asymptotic estimates are generally difficult. However, in several interesting cases, the linear forms $p_{hn} - q_n v_h$ can be expressed by multiple integrals of n-th powers of suitable rational functions, whereas the common coefficients q_n are expressed by multiple integrals of the same integrands, taken over the product of closed contours (see, e.g., [5]).

Thus the analytic representation of the linear forms and of the common coefficients is naturally related to the theory of periods (following Kontsevich and Zagier [3], for example), while the required estimates for $|p_{hn} - q_n v_h|$ and $|q_n|$ can be obtained through the asymptotic evaluation, as $n \to +\infty$, of multiple complex integrals. A natural way to achieve the latter is the use of a suitable extension to any dimension N of the classical saddle-point method in $\mathbb{C}$.

The problem of extending the saddle-point method to multiple integrals

$$\int_{\Gamma} f(z_1, \dots, z_N)^n g(z_1, \dots, z_N)\, dz_1 \dots dz_N$$

over suitable manifolds $\Gamma \subset \mathbb{C}^N$ with $N > 1$ was studied by M. V. Fedoryuk [1]. This author was primarily interested in a constructive process to transform the integration manifold Γ into a manifold Λ of 'steepest descent' for $|f(z_1, \dots, z_N)|$ containing a saddle-point of $f(z_1, \dots, z_N)$ and preserving the value of the integral. For the purpose of constructing Λ, Fedoryuk introduced techniques from algebraic topology based on homology groups which, beside their theoretical interest, proved to be difficult to apply in concrete examples. In fact, in an example of dimension $N = 2$, Ursell [4] showed the non-uniqueness of steepest descent surfaces, with the result that in most cases there is no available criterion to find towards which saddle-point the surface of integration should be deformed.

In [2] Hata introduced new ideas to circumvent such difficulties in the two-dimensional case. Using a more flexible analytic method, essentially consisting in a double reduction to the one-dimensional case, Hata proved an asymptotic formula for a double integral

$$\iint_{\lambda_1 \times \lambda_2} f(z_1, z_2)^n g(z_1, z_2)\, dz_1\, dz_2 \qquad (n \to +\infty),$$

where f and g are holomorphic functions in an open set $\Delta \subset \mathbb{C}^2$, λ_1 and λ_2 are paths with $\lambda_1 \times \lambda_2 \subset \Delta$, and $n \in \mathbb{N}$.

In joint work with F. Pinna (to appear) we have generalised Hata's analytic method to the higher dimensional case, by proving a version of the saddle-point method in $\mathbb{C}^N$ for any $N \geq 2$. Our result is based on the notion of 'admissible' saddle-point of f defined below, which is not essentially restrictive.

Let $f(z_1, \ldots, z_N)$ be holomorphic in an open set $\Delta \subset \mathbb{C}^N$. We consider the following partial hessian determinants with respect to the ordering $z_1, \ldots, z_N$ of the variables:

$$H_j(z_1, \ldots, z_N) = \begin{vmatrix} \frac{\partial^2 f}{\partial z_1^2} & \cdots & \frac{\partial^2 f}{\partial z_1 \partial z_j} \\ \vdots & \ddots & \vdots \\ \frac{\partial^2 f}{\partial z_j \partial z_1} & \cdots & \frac{\partial^2 f}{\partial z_j^2} \end{vmatrix} \qquad (j = 1, \ldots, N),$$

and we denote by

$$H(z_1, \ldots, z_N) = H_N(z_1, \ldots, z_N)$$

the hessian determinant of f.

Definition 1. The point $\big(z_1^{(0)}, \ldots, z_N^{(0)}\big) \in \Delta$ is an admissible saddle-point of f with respect to the ordering $z_1, \ldots, z_N$ of the variables if

$$\begin{cases} f\big(z_1^{(0)}, \ldots, z_N^{(0)}\big) \neq 0 \\ \frac{\partial f}{\partial z_j}\big(z_1^{(0)}, \ldots, z_N^{(0)}\big) = 0 \quad (j = 1, \ldots, N) \\ H_j\big(z_1^{(0)}, \ldots, z_N^{(0)}\big) \neq 0 \quad (j = 1, \ldots, N). \end{cases}$$

Let $\big(z_1^{(0)}, \ldots, z_N^{(0)}\big)$ be an admissible saddle-point of f with respect to the ordering $z_1, \ldots, z_N$. By the implicit function theorem, for each $j = 1, \ldots, N-1$ the system

$$\frac{\partial f}{\partial z_1} = \cdots = \frac{\partial f}{\partial z_j} = 0$$

is locally solvable with respect to $z_1, \ldots, z_j$. Accordingly, let

$$z_1 = Z_{1j}(z_{j+1}, \ldots, z_N), \ \ldots, \ z_j = Z_{jj}(z_{j+1}, \ldots, z_N)$$

be the implicit functions satisfying the identities

$$\begin{cases} \frac{\partial f}{\partial z_1}\big(Z_{1j}(z_{j+1}, \ldots, z_N), \ \ldots, \ Z_{jj}(z_{j+1}, \ldots, z_N), \ z_{j+1}, \ \ldots, \ z_N\big) = 0 \\ \quad \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \\ \frac{\partial f}{\partial z_j}\big(Z_{1j}(z_{j+1}, \ldots, z_N), \ \ldots, \ Z_{jj}(z_{j+1}, \ldots, z_N), \ z_{j+1}, \ \ldots, \ z_N\big) = 0 \end{cases}$$

in a neighbourhood of $\big(z_1^{(0)}, \ldots, z_N^{(0)}\big)$. In order to apply the saddle-point method to an N-fold multiple integral, using Cauchy's theorem we change the N integration paths into new paths $\lambda_1, \ldots, \lambda_N$ as follows. For $n = 1, 2, 3, \ldots$ let

$$I_n = \int\limits_{\lambda_N} dz_N \int\limits_{\lambda_{N-1}(z_N)} dz_{N-1} \cdots \int\limits_{\lambda_2(z_3, \ldots, z_N)} dz_2 \int\limits_{\lambda_1(z_2, \ldots, z_N)} f(z_1, \ldots, z_N)^n g(z_1, \ldots, z_N)\, dz_1$$

be an absolutely convergent N-fold integral, with $g(z_1,\dots,z_N)$ holomorphic in Δ. Let $\big(z_1^{(0)},\dots,z_N^{(0)}\big)$ be an admissible saddle-point of f with respect to the ordering $z_1,\dots,z_N$, at which $g\big(z_1^{(0)},\dots,z_N^{(0)}\big)\neq 0$. For $j=1,\dots,N-1$, denote

$$\widetilde{f}_j(z_{j+1},\dots,z_N) := f\big(Z_{1j}(z_{j+1},\dots,z_N),\ \dots,\ Z_{jj}(z_{j+1},\dots,z_N),\ z_{j+1},\ \dots,\ z_N\big).$$

We assume $z_N^{(0)}\in\lambda_N$, and $\big|\widetilde{f}_{N-1}(z_N)\big| < \big|f\big(z_1^{(0)},\dots,z_N^{(0)}\big)\big|$ for $z_N\in\lambda_N$ in a neighbourhood of $z_N^{(0)}$, $z_N\neq z_N^{(0)}$. Similarly, in a neighbourhood of $\big(z_1^{(0)},\dots,z_N^{(0)}\big)$, for each $j=1,\dots,N-1$ and for any fixed $(z_{j+1},\dots,z_N)$ with $z_N\in\lambda_N$, $\dots$, $z_{j+1}\in\lambda_{j+1}(z_{j+2},\dots,z_N)$, we assume $Z_{jj}(z_{j+1},\dots,z_N)\in\lambda_j(z_{j+1},\dots,z_N)$ and $\big|\widetilde{f}_{j-1}(z_j,z_{j+1},\dots,z_N)\big| < \big|\widetilde{f}_j(z_{j+1},\dots,z_N)\big|$ for $z_j\in\lambda_j(z_{j+1},\dots,z_N)$, $z_j\neq Z_{jj}(z_{j+1},\dots,z_N)$, where $\widetilde{f}_0:=f$. The above assumptions imply

$$|f(z_1,\dots,z_N)| < \big|f\big(z_1^{(0)},\dots,z_N^{(0)}\big)\big|$$

for all $(z_1,\dots,z_N)\neq\big(z_1^{(0)},\dots,z_N^{(0)}\big)$ in a neighbourhood of $\big(z_1^{(0)},\dots,z_N^{(0)}\big)$ such that $z_N\in\lambda_N$, $\dots$, $z_1\in\lambda_1(z_2,\dots,z_N)$. We require that such a maximality condition holds also away from $\big(z_1^{(0)},\dots,z_N^{(0)}\big)$. We assume that for any neighbourhood σ of $\big(z_1^{(0)},\dots,z_N^{(0)}\big)$ there exists a real number $\mu=\mu(\sigma)$ with $0<\mu<1$ such that

$$|f(z_1,\dots,z_N)| \le \mu\big|f\big(z_1^{(0)},\dots,z_N^{(0)}\big)\big|$$

for all $z_N\in\lambda_N$, $\dots$, $z_1\in\lambda_1(z_2,\dots,z_N)$ satisfying $(z_1,\dots,z_N)\notin\sigma$.

Theorem 1. Under the assumptions above, for $n\to+\infty$ the asymptotic formula

$$I_n = (2\pi)^{N/2}\,e^{i(\vartheta_1+\cdots+\vartheta_N)}\,g\big(z_1^{(0)},\dots,z_N^{(0)}\big)\,\frac{\big|f\big(z_1^{(0)},\dots,z_N^{(0)}\big)\big|^{N/2}}{\sqrt{\big|H\big(z_1^{(0)},\dots,z_N^{(0)}\big)\big|}} \times \frac{f\big(z_1^{(0)},\dots,z_N^{(0)}\big)^n}{n^{N/2}}\left(1+O\left(\frac{(\log n)^{\frac{3}{2}+\varepsilon}}{\sqrt{n}}\right)\right)$$

holds for any $\varepsilon>0$, where, for $j=1,\dots,N$,

$$\vartheta_j = h_j\pi - \frac{1}{2}\arg\left(-\frac{1}{f\big(z_1^{(0)},\dots,z_N^{(0)}\big)}\cdot\frac{H_j\big(z_1^{(0)},\dots,z_N^{(0)}\big)}{H_{j-1}\big(z_1^{(0)},\dots,z_N^{(0)}\big)}\right),$$

with $h_j\in\mathbb{Z}$. Here $H_0(z_1,\dots,z_N):=1$.

References

[1] M. V. Fedoryuk, *Metod perevala*, Nauka, Moscow, 1977 (Russian).

[2] M. Hata, *$\mathbb{C}^2$-saddle method and Beukers' integral*, Trans. Amer. Math. Soc. **352** (2000), 4557–4583.

[3] M. Kontsevich and D. Zagier, *Periods*, in: *Mathematics unlimited – 2001 and beyond*, Springer-Verlag (2001), 771–808.

[4] F. Ursell, *Integrals with a large parameter: a double complex integral with four nearly coincident saddle-points*, Math. Proc. Cambridge Phil. Soc. **87** (1980), 249–273.

[5] C. Viola and W. Zudilin, *Linear independence of dilogarithmic values*, J. reine angew. Math., http://dx.doi.org/10.1515/crelle-2015-0030

An application of Diophantine approximation to regularity of patterns in cut and project sets

Alan Haynes

(joint work with Henna Koivusalo, James Walton)

As the title indicates, in this talk we discussed an application of Diophantine approximation to the study of regularity of patterns in cut and project sets. Cut and project sets are point sets in Euclidean space which arise from a simple dynamical construction: they are the return times, to specified regions, of linear $\mathbb{R}^d$ actions on higher dimension tori.

Under mild assumptions, cut and project sets are typically Delone sets which are aperiodic (i.e. their group of translational periods is $\{0\}$). They are important for a number of reasons, and have been studied extensively in recent years because of their potential as mathematical models for physical materials called quasicrystals. Many well known aperiodic patterns in Euclidean space, for example the collections of vertices of any Penrose or Ammann-Beenker tiling, can be constructed using cut and project sets.

As a point of reference, one dimensional cut and project sets correspond in a very natural way, by well known work of Morse and Hedlund [5], to Sturmian words (aperiodic bi-infinite words on a two letter alphabet with minimal growth of word complexity). Higher dimensional aperiodic cut and project sets may or may not have minimal pattern complexity.

For point patterns $Y \subseteq \mathbb{R}^d$, another measurement of pattern regularity is given by the repetitivity function $R : [1, \infty) \to [0, \infty)$. For each $r \geq 1$, the quantity $R(r)$ is defined to be the smallest real number with the property that every pattern of size r, which occurs anywhere in Y, occurs in every ball of radius $R(r)$ in $\mathbb{R}^d$. If there is a constant $C > 0$ with the property that $R(r) < Cr$ for all $r \geq 1$, then Y is called linearly repetitive (LR). In general, linear repetitivity implies minimal pattern complexity, but the converse is far from true. For Sturmian words, linear repetitivity is equivalent to 'badly approximable slope' [5, p.2].

The main problem which we focused on in this talk was the problem of characterizing the collection of LR cut and project sets. This problem was originally posed by Lagarias and Pleasants [4, Problem 8.3], who promoted linearly repetitive cut and project sets as models for 'perfectly ordered quasicrystals.' Our main result focuses on totally irrational, aperiodic and non-singular cut and project sets formed with cubical acceptance domains. To give the impression of our results, we present them here. However, we do not attempt to provide all of the definitions and instead refer to [2] for a complete exposition.

Theorem 1. A k to d cubical cut and project set defined by linear forms $\{L_i\}_{i=1}^{k-d}$ is LR if and only if

(LR1) The sum of the ranks of the kernels of the maps $\mathcal{L}_i : \mathbb{Z}^d \to \mathbb{R}/\mathbb{Z}$ defined by

$$\mathcal{L}_i(n) = L_i(n) \bmod 1$$

is equal to $d(k-d-1)$, and

(LR2) Each L_i is relatively badly approximable.

Condition (LR1) is necessary and sufficient for Y to have minimal pattern complexity. For comparison, in [3, Section 5] it was shown that minimal pattern complexity is a necessary and sufficient condition for the Čech cohomology (with rational coefficients) of the associated tiling space to be finitely generated. Many of the calculations in the first part of our proof of this theorem share a common thread with those that arise in the calculation of the cohomology groups. This point of view eventually leads us to a collection of equations (equations (3.3)-(3.6) in [2]) which form the crux of our argument, allowing us to move directly in our proof to a position where we can apply condition (LR2). It should be pointed out that, without the group theoretic arguments that give us the rigid structure imposed by the mentioned equations, the proof would fall apart.

Condition (LR2) is a Diophantine condition, which places a strong restriction on how well the subspace defining Y can be approximated by rationals. We define a linear form to be relatively badly approximable if it is badly approximable when restricted to rational subspaces complementary to its kernel. Note that in the special case when $k - d = 1$, condition (LR1) is automatically satisfied, and condition (LR2) requires the linear form defining Y to be badly approximable in the usual sense. This observation allows us to give, as a corollary, a complete characterization of both cubical and canonical (another important class in the study of quasicrystals) cut and project sets in codimension 1, extending a classical theorem of Morse and Hedlund [5, p.2].

At the end of the talk, we discussed in more detail the relationship between cubical cut and project sets and their canonical counterparts (i.e. for arbitrary dimension and codimension). In many cases which are commonly cited in the literature, our results for cubical cut and project sets also apply to canonical ones. However, what is possibly more interesting is that there are examples of LR cubical cut and project sets which are no longer LR when their acceptance domains are replaced by canonical ones.

There are at least two seemingly different sources for this type of behavior. The first is geometric, and arises in the situation when at least two of the linear forms defining the physical space have co-kernels with different ranks. The second (which can occur even in the absence of the geometric situation just described) is Diophantine, and is related to the fact that any number can be written as a product of two badly approximable numbers (this follows from Marshall Hall's famous theorems in [1]). In [2, Problem 4.5] we propose a line of thought which should lead to a more complete understanding and characterization of linearly repetitive canonical cut and project sets.

It should be pointed out that most canonical cut and project sets of specific interest in the literature arise from subspaces defined by linear forms with coefficients in a fixed algebraic number field. In such a case the Diophantine behavior alluded to in the previous paragraph cannot occur. To illustrate this point, in [2] we also explain how to prove that Penrose and Ammann-Beenker tilings are LR. This in itself is not a new result, and in fact it is follows quickly from descriptions of these tilings using substitution rules. What is new is that our proof uses only their descriptions as cut and project sets.

References

[1] M. J. Hall: *On the sum and product of continued fractions*, Ann. of Math. (2) 48 (1947), 966–993.

[2] A. Haynes, H. Koivusalo, J. Walton: *A characterization of linearly repetitive cut and project sets*, preprint, `arXiv:1503.04091`.

[3] A. Julien: *Complexity and cohomology for cut-and-projection tilings*, Ergodic Theory Dyn. Syst. 30 (2010), no. 2, 489–523.

[4] J. C. Lagarias, P. A. B. Pleasants: *Repetitive Delone sets and quasicrystals*, Ergodic Theory Dynam. Systems 23 (2003), no. 3, 831–867.

[5] M. Morse, G. A. Hedlund: *Symbolic dynamics II. Sturmian trajectories*, Amer. J. Math. 62 (1940), 1–42.

How should potential counterexamples to p-adic Littlewood conjecture look like?

Dzmitry Badziahin

In 2004 de Mathan and Teulie proposed the following problem which is now called Mixed Littlewood Conjecture (MLC). Before stating it we need to introduce some notation. Let $\mathcal{D} := \{d_i\}_{i\in\mathbb{N}}$ be a sequence of positive integers with $d_i \geq 2$. Let $D_n := \prod_{i=1}^{n} d_i$. Then the pseudonorm $|a|_{\mathcal{D}}$ of an integer number a is defined as follows:

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

The Mixed Littlewood Conjecture (MLC) in its full generality states the following.

Conjecture 1. For any sequence $\mathcal{D}$ of positive integers not smaller than two and for any $x \in \mathbb{R}$ we have

$$\liminf_{q\to\infty} q \cdot |q|_{\mathcal{D}} \cdot ||qx|| = 0.$$

If $\mathcal{D}$ is a constant sequence consisting of a prime p then the pseudonorm $|a|_{\mathcal{D}}$ becomes the standard p-adic norm. The MLC for this particular sequence has a special name: the p-adic Littlewood conjecture (PLC).

In this report we will concentrate on what we know about the conjectures and the conditions of their counterexamples x (if they exist).

Concerning MLC in its full generality, although it is still open, there are some reasonable concerns that it is probably false. For example by developing the theory of generalised Cantor-winning sets we can prove the following (see [3]).

Theorem 1 (B., Harrap, 2014)**.** For an arbitrary function $f : \mathbb{N} \to \mathbb{R}_{\geq 0}$ such that $\lim_{q\to\infty} f(q) = \infty$ there exists a sequence $\mathcal{D}$ such that the set of $x \in \mathbb{R}$ for which

$$\liminf_{q\to\infty} f(q)q \cdot |q|_{\mathcal{D}} \cdot ||qx|| > 0$$

has full Hausdorff dimension.

In other words, however slowly growing $f(q)$ is we can construct a sequence $\mathcal{D}$ such that MLC, weakened by the factor $f(q)$ becomes false for a quite large set of real numbers x. Moreover, in [3] we just have precise conditions on $\mathcal{D}$ which allow us to state the theorem: it should grow fast enough.

On the other hand PLC is generally believed to be true.

Today we know two generalisations of PLC, they are quite closely related, and each of them has their advantages. The first one was suggested by Einsiedler and Kleinbock in 2007 [5].

Conjecture 2 (EK)**.** For any $(u, v) \in \mathbb{R} \times \mathbb{Q}_p$ and any prime p one has

$$\liminf \max\{|q_0|, |q|\}|qu - q_0| \cdot |qv - q_0|_p = 0.$$

One can check that the Conjecture EK implies PLC by the following (not trivial) assertion: Conjecture EK for $(u, 0)$ implies PLC for $x = u^{-1}$.

This conjecture has close links with the dynamics on the space of lattices in $\mathbb{R}^2 \times \mathbb{Q}_p^2$. By using this link and the ideas developed by Einsiedler, Kleinbock and Lindenstrauss one can show that the set of counterexamples to EK conjecture is very small.

Theorem 2 (B. Bugeaud, Einsielder, Kleinbock)**.** The set (u, v) of counterexamples to EK conjecture has Hausdorff dimension zero.

On the other hand the set of counterexamples is not empty.

Theorem 3 (B.)**.** Let $u \in \mathbb{R}$ and $v \in \mathbb{Q}_p$ be irrational solutions of the same quadratic equation. Then they form a counterexample to EK conjecture.

The last theorem is not as extraordinary as one may think. Such pairs (u, v) are related with periodic orbits in the space of lattices in $\mathbb{R}^2 \times \mathbb{Q}_p^2$. We refer the reader to [5, 2] for more details.

Another generalisation [1] can be formulated as follows. Let $E := \mathcal{A}_n^{\mathbb{N}} \times \mathbb{P}^1_{\mathbb{Q}_p}$ where $\mathcal{A}_n := \{1, \dots, n\}$. In other words E is the set of pairs: an infinite word over a finite alphabet and a one-dimensional projective p-adic point. Define

$$T : E \to E; \quad T(a_0a_1, \dots, \mathbf{q}) \mapsto (a_1a_2 \dots, A_{a_0}\mathbf{q}),$$

where

$$A_a = \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}.$$

Define the set of p-adically badly approximable points as follows

$$\mathbf{PBad}_\epsilon := \{\mathbf{q} \in \mathbb{P}^1_{\mathbb{Q}_p} \ : \ \forall \mathbf{a} \in \mathbb{Z}^2, |(\mathbf{a}, \mathbf{q})|_p \geq \epsilon ||\mathbf{q}||_p ||\mathbf{a}||^{-2}.$$

Finally we define

$$\mathbf{LBad} := \{\mathbf{x} \in E \ : \ \exists \epsilon > 0, \forall n \in \mathbb{N}, T^n\mathbf{x} \in \mathcal{A}_n^{\mathbb{N}} \times \mathbf{PBad}_\epsilon\}.$$

The counterexamples to PLC are related with the set **LBad** in the following way. For a given badly approximable x take an element $\mathbf{x} := (w_{CF}(x), \binom{1}{0}) \in E$. Then x is a counterexample to PLC if every limit point of the sequence $\{T^n\mathbf{x}\}_{n\in\mathbb{N}}$ is in **LBad**.

Unfortunately we can prove that **LBad** is nonempty.

Theorem 4 (B.)**.** Let $w = (\overline{p})$ be a periodic word with a period p. Let $\mathbf{q} \in \mathbb{P}^1_{\mathbb{Q}_p}$ be such that $A_p\mathbf{q} = \mathbf{q}$. Then $(w, \mathbf{q}) \in \mathbf{LBad}$.

Bugeaud, Drmota and de Mathan showed that the elements of **LBad** from this theorem can not generate a counterexample to PLC. In 2004 they proved the following theorem (which was formulated in different terms, see[4]).

Theorem 5 (Bugeaud, Drmota, de Mathan)**.** If one of the limit points of $\{T^n w_{CF}(x)\}_{n\in\mathbb{N}}$ is periodic then x satisfies PLC.

One can hope that **LBad** does not have any other elements. If one can prove that then PLC will follow automatically. We formalise this in the following conjecture.

Conjecture 3 (B)**.** For every element $(w, \mathbf{q})$ of **LBad** the orbit $T^n(w, \mathbf{q})$ is periodic.

The results in [1] contain quite restrictive and technical conditions on the elements of **LBad**. One of the more or less nice corollaries from them is the following theorem.

Theorem 6 (B)**.** If w is not periodic and for some constant C the subword complexity of w satisfies $P(w, n) - n < C$ then for every $\mathbf{q} \in \mathbb{P}^1_{\mathbb{Q}_p}$, we have $(w, \mathbf{q}) \notin \mathbf{LBad}$.

References

[1] D. Badziahin, *On continued fraction expansion of potential counterexamples to p-adic Littlewood conjecture*, Preprint, `http://arxiv.org/abs/1406.3594`

[2] D. Badziahin, Y. Bugeaud, M. Einsiedler, D. Kleinbock, *On the mixed Littlewood conjecture*, Compositio Math., **151(9)** (2015), 1647–1662.

[3] D. Badziahin, S. Harrap, *Cantor-winning sets and their applications*, Preprint, `http://arxiv.org/abs/1503.04738`

[4] Y. Bugeaud, M. Drmota, B. de Mathan, *On a mixed Littlewood conjecture in Diophantine approximation*, Acta Arith. **128** (2007), 107–124.

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

Integral points and the Shafarevich conjecture for abelian surfaces

Aaron Levin

The Shafarevich conjecture for curves, proved by Faltings [4], states that given a number field k, integer $g \geq 2$, and finite set of primes S of k, there are only finitely many isomorphism classes of nonsingular projective curves C over k of genus g with good reduction outside S. More generally, Faltings [4] proved an analogous result for abelian varieties.

Theorem 1 (Shafarevich conjecture for principally polarized abelian varieties)**.** Given a number field k, positive integer g, and finite set of primes S of k, there are only finitely many isomorphism classes of principally polarized abelian varieties over k of dimension g with good reduction outside S.

Using an appropriate version of Torelli's theorem, Theorem 1 implies the Shafarevich conjecture for curves. The Shafarevich conjecture for curves implies, via a construction of Parshin [10], the truth of the Mordell conjecture: If C is a curve defined over a number field k of (geometric) genus $g(C) \geq 2$, then the set of k-rational points $C(k)$ is finite. While both the Shafarevich conjecture and the Mordell conjecture are now theorems (of Faltings), a major defect of both theorems is that there is no known effective proof of either result, that is, there is no known algorithm to (provably) find the finitely many objects in the conclusion of either theorem.

It is known that an effective version of the Shafarevich conjecture implies an effective version of the Mordell conjecture, and an explicit relationship has been given by Rémond [12]. In fact, even effective versions of restricted forms of the Shafarevich conjecture have deep consequences. Recall Siegel's theorem on integral points on curves:

Theorem 2 (Siegel)**.** Let C be a curve over k and $\phi \in k(C)$ a nonconstant rational function on C. If C is a rational curve then assume further that ϕ has at least three distinct poles. The set of S-integral points of C with respect to ϕ,

$$\{P \in C(k) \mid \phi(P) \in \mathcal{O}_{k,S}\},$$

is finite.

Using the theory of linear forms in logarithms, if the curve C has genus zero or genus one, then Siegel's theorem is known to be effective (for every choice of ϕ, k, and S) by work of Baker and Coates [1] (see also [11]). Already for curves of genus two, however, no general effective version of Siegel's theorem is known. In this case, for certain special choices of ϕ, Siegel's theorem has been proven in an effective way. For instance, if ϕ contains a Weierstrass point as a pole, or a pair of points conjugate under the hyperelliptic involution as poles, then the theory of linear forms in logarithms again yields an effective version of Siegel's theorem for ϕ (and any k and S). Thus, the genus two case of Siegel's theorem represents the simplest open case of Siegel's theorem with respect to effectivity.

In [8], I proved a relation between an effective Shafarevich conjecture for hyperelliptic Jacobians (i.e., Jacobians of hyperelliptic curves) and an effective version of Siegel's theorem for hyperelliptic curves.

Theorem 3. Let $g \geq 2$. Suppose that for every number field k and every finite set of places S of k, one can effectively compute the isomorphism classes of hyperelliptic Jacobians of dimension g with good reduction outside S (e.g., by computing a set of explicit hyperelliptic Weierstrass equations). Then Siegel's Theorem is effective for every hyperelliptic curve of genus g (and all choices of ϕ, k, and S).

In particular, an effective Shafarevich conjecture for abelian surfaces would imply an effective version of Siegel's theorem for curves of genus two. Thus, aside from its intrinsic interest, an effective Shafarevich conjecture for abelian surfaces has deep Diophantine consequences. To study the Shafarevich conjecture for abelian surfaces, we begin by recalling the structure of principally polarized abelian surfaces over a number field k.

Theorem 4 (González-Guàrdia-Rotger [6])**.** Let k be a number field and let A be a principally polarized abelian surface over k. Then (as a polarized abelian variety) A is isomorphic over k to one of the following:

(1) The Jacobian $\mathrm{Jac}(C)$ of a genus 2 curve C over k.
(2) $E_1 \times E_2$, where E_1 and E_2 are elliptic curves over k.
(3) $W = \mathrm{Res}_{k'/k} E$, where W is the Weil restriction of an elliptic curve E over a quadratic extension k'/k.

Using standard facts about bad reduction of products and Weil restrictions of abelian varieties, the Shafarevich conjecture in the last two cases is easily reduced to the Shafarevich conjecture for elliptic curves, which is effective by work of Coates [2] (explicit results have been proven by Fuchs, von Känel, and Wüstholz [4]). Thus, proving an effective Shafarevich conjecture for abelian surfaces reduces to proving an effective Shafarevich conjecture for Jacobians of genus two curves.

We note that the Shafarevich conjecture for hyperelliptic curves is known in an effective way. Building on work of Evertse and Győry [3], von Känel [7] proved explicit bounds for the heights of Weierstrass models of the involved hyperelliptic curves. Recall that if a nonsingular projective curve C has good reduction at a prime $\mathfrak{p}$, then the Jacobian $\mathrm{Jac}(C)$ also has good reduction at the prime $\mathfrak{p}$. The primes for which the converse statement fails appear to hold the key to proving an effective Shafarevich conjecture for hyperelliptic Jacobians. We make the following definition.

Definition 1. Let C be a nonsingular projective curve over a number field k. If a prime $\mathfrak{p}$ of $\mathcal{O}_k$ is simultaneously a prime of bad reduction for C and a prime of good reduction for the Jacobian $\mathrm{Jac}(C)$, then we call $\mathfrak{p}$ a Janus prime for C (or $\mathrm{Jac}(C)$).

With this terminology, we prove a result towards an effective Shafarevich conjecture for Jacobians of genus two curves.

Theorem 5. Let k be a number field and let S be a finite set of primes of k. Then one can effectively compute, up to isomorphism, all genus two curves C over k such that $A = \mathrm{Jac}(C)$ satisfies:

(1) A has good reduction outside S.
(2) A has at most two Janus primes outside S.
(3) A has full rational 2-torsion.

The first ingredient in the proof of the theorem is an algorithm of Liu [9] to compute, given a Weierstrass equation for a genus two curve, the fibers of a minimal model of the curve (away from primes above 2, at least). This allows us to study genus two curves C of a very specific explicit form. We then reduce the problem to certain Diophantine equations which can be handled by the combination of a version of Runge's method and (effective) S-unit equation analysis.

References

[1] A. Baker and J. Coates, *Integer points on curves of genus 1*, Proc. Cambridge Philos. Soc. **67** (1970), 595–602.
[2] J. Coates, *An effective p-adic analogue of a theorem of Thue. III. The diophantine equation* $y^2 = x^3 + k$, Acta Arith. **16** (1969/1970), 425–435.
[3] J.-H. Evertse and K. Győry, *Effective finiteness results for binary forms with given discriminant*, Compositio Math. **79** (1991), no. 2, 169–204.
[4] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366.
[5] C. Fuchs, R. von Känel, and G. Wüstholz, *An effective Shafarevich theorem for elliptic curves*, Acta Arith. **148** (2011), no. 2, 189–203.
[6] J. González, J. Guàrdia, and V. Rotger, *Abelian surfaces of* GL_2*-type as Jacobians of curves*, Acta Arith. **116** (2005), no. 3, 263–287.
[7] R. von Känel, *An effective proof of the hyperelliptic Shafarevich conjecture*, J. Théor. Nombres Bordeaux **26** (2014), no. 2, 507–530.
[8] A. Levin, *Siegel's theorem and the Shafarevich conjecture*, J. Théor. Nombres Bordeaux **24** (2012), no. 3, 705–727.
[9] Q. Liu, *Modèles minimaux des courbes de genre deux*, J. Reine Angew. Math. **453** (1994), 137–164.
[10] A. N. Parshin, *Minimal models of curves of genus* 2*, and homomorphisms of abelian varieties defined over a field of finite characteristic*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 67–109.
[11] D. Poulakis, *Points entiers sur les courbes de genre* 0, Colloq. Math. **66** (1993), no. 1, 1–7.
[12] G. Rémond, *Hauteurs thêta et construction de Kodaira*, J. Number Theory **78** (1999), no. 2, 287–311.

Many Thue equations have no solutions

Shabnam Akhtari
(joint work with Manjul Bhargava)

It is not very difficult to construct binary forms that do not represent a given integer, if we arrange a local obstruction. For example, any binary cubic form congruent to $xy(x + y)$ modulo 2 will never represent an odd number. Also, if $F(x, y) = 1$ has no solution, and G is a *proper subform* of F, i.e., $G(x, y) =$

$F(ax+by, cx+dy)$ for some integer matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $|\det A| > 1$, then clearly $G(x,y) = 1$ will also have no integer solutions.

In [1] we show for every integer $n \geq 3$ that many (indeed, a positive proportion) of binary forms of degree n are not proper subforms, locally represent 1 at every place, but globally fail to represent 1.

Theorem 1 (Akhtari and Bhargava)**.** Let h be any nonzero integer. When $\mathrm{GL}_2(\mathbb{Z})$-classes of integral binary cubic forms $F(x,y) \in \mathbb{Z}[x,y]$ are ordered by absolute discriminant, a positive proportion of these forms F have the following properties:

(1) they locally everywhere represent h (i.e., $F(x,y) = h$ has a solution in $\mathbb{R}^2$ and in $\mathbb{Z}_p^2$ for all p);
(2) they globally do not represent h (i.e., $F(x,y) = h$ has no solution in $\mathbb{Z}^2$); and
(3) they are maximal forms (i.e., F is not a proper subform of any other form).

Our method of proof provides an explicit lower bound for the positive density of classes of binary cubic forms that do not represent a given integer, and indeed an explicit construction of this positive density of forms. Our strategy to prove Theorem 1 is as follows. We first construct a set of maximal binary cubic forms $F(x,y)$ of positive density defined by congruence conditions. For any such irreducible binary cubic form $F(x,y)$ of sufficiently large discriminant, we show that each solution of $F(x,y) = m$ corresponds uniquely to a solution of $G_j(x,y) = h$, where G_j lies in a certain set of 81 maximal binary cubic forms $G_j(x,y) = h$ associated to F with $\mathrm{Disc}(G_j) \ll \mathrm{Disc}(F)$, and $m \in \mathbb{Z}$ is a suitably chosen positive multiple of h. These G_j's are constructed using the polynomial congruence results that are introduced in [3] and [4]. Using the fact that F can represent m only an absolutely bounded number of times by Proposition 1, which is a main result of [2], we conclude that most of the G_j's cannot represent h.

Proposition 1 (Akhtari, 2015)**.** Let $F(x,y) \in \mathbb{Z}[x,y]$ be an irreducible binary form of degree $n \geq 3$ and discriminant D. Let m be an integer with

$$0 < m \leq \frac{|D|^{\frac{1}{2(n-1)}-\epsilon}}{(3.5)^{n/2} n^{\frac{n}{2(n-1)}}},$$

where $0 < \epsilon < \frac{1}{2(n-1)}$. Then the equation $F(x,y) = m$ has at most

$$\begin{cases} 7n + \frac{n}{(n-1)\epsilon} & \text{if } n \geq 5 \\ 9n + \frac{n}{(n-1)\epsilon} & \text{if } n = 3, 4 \end{cases}$$

primitive solutions. (If n is even, then two solutions (x_0, y_0) and $(-x_0, -y_0)$ are considered here to be one solution).

In [1], we also show an analogous result for binary forms of general degree, provided that these forms are ordered by the maximum of the absolute values of their coefficients.

Theorem 2 (Akhtari and Bhargava)**.** Let h be any nonzero integer. When binary forms $F(x,y) \in \mathbb{Z}[x,y]$ of a given degree $n \geq 3$ are ordered by the maximum of absolute values of their coefficients, a positive proportion of them have the following properties:

(1) they locally everywhere represent h (i.e., $F(x,y) = h$ has a solution in $\mathbb{R}^2$ and in $\mathbb{Z}_p^2$ for all p);
(2) they globally do not represent h (i.e., $F(x,y) = h$ has no solution in $\mathbb{Z}^2$); and
(3) they are maximal forms (i.e., F is not a proper subform of any other form).

As with Theorem 1, our method of proof provides an explicit lower bound for the positive density of binary n-ic forms that do not represent a given integer, and moreover, yields an explicit construction of this positive density of forms. Since, unlike the case $n = 3$, asymptotics for the number $\mathrm{GL}_2(\mathbb{Z})$-classes of binary n-ic forms of bounded discriminant are not known for $n > 3$, we instead order all integral binary n-ic forms by the maximum of the absolute values of their coefficients, but otherwise follow a strategy analogous to that of the cubic case in Theorem 1.

References

[1] S. Akhtari and M. Bhargava, *A positive proportion of locally soluble Thue equations are globally insoluble*, arXiv:1603.08623.
[2] S. Akhtari, *Representation of small integers by binary forms*, Q. J. Math **66** (4) (2015), 1009–1054.
[3] E. Bombieri, W. M. Schmidt, *On Thue's equation*, Invent. Math. **88** (1987), 69-81.
[4] C. L. Stewart, *On the number of solutions of polynomial congruences and Thue equations*, Journal of American Math. Soc. **4** (1991), 793–838.

Lower bounds for the height in Galois extension

Francesco Amoroso
(joint work with David Masser)

Let α be a non zero algebraic number of degree d which is not a root of unity. We denote by $h(\alpha)$ the usual logarithmic Weil height which is, by a well-known result of Kronecker, > 0. In 1933 Lehmer asked ("Lehmer Problem") if there exists a positive real number c such that $h(\alpha) > cd^{-1}$. This should be the best possible lower bound for the height (without any further assumption on α), since $h(2^{1/d}) = (\log 2)d^{-1}$. The best known result in the direction of the Lehmer Problem is Dobrowolski's lower bound, which implies that for any $\varepsilon > 0$ there is $c(\varepsilon) > 0$ such that $h(\alpha) \geq c(\varepsilon)d^{-1-\varepsilon}$.

The inequality in the Lehmer Problem has been established in some special cases. For instance it was proved by Symth [8] for non-reciprocal α (in particular whenever d is odd). Also, Mignotte (see [7]) gives a positive answer if there exists a prime $p \leq d \log d$ which splits completely in $\mathbb{Q}(\alpha)$. More recently, Lehmer Problem

was solved by Borwein, Dobrowolski and Mossinghoff (see [3]) for algebraic integers whose minimal polynomial has coefficients all congruent to 1 modulo a fixed $m \geq 2$.

David and the author of this talk (see [1], *Corollaire 1.7*) proved Lehmer Problem when $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a Galois extension. We improve on the result in the Galois case, and we even show that for any $\varepsilon > 0$ there is $c(\varepsilon) > 0$ such that

$$h(\alpha) \geq c(\varepsilon) d^{-\varepsilon}$$

when $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a Galois extension.

Our main results are the following:

Theorem 1. For any integer $r \geq 1$ and any $\varepsilon > 0$ there is a positive effective constant $c(r, \varepsilon)$ with the following property. Let $\mathbb{F}/\mathbb{Q}$ be a Galois extension of degree D and $\alpha \in \mathbb{F}^*$. We assume that there are r conjugates of α over $\mathbb{Q}$ which are multiplicatively independent[1]. Then

$$h(\alpha) \geq c(r, \varepsilon) D^{-1/(r+1)-\varepsilon}.$$

The proof builds on the method of [1] and on a more recent result of [4], which in turns generalizes both the main result of [1] and the Relative Dobrowolki Theorem of [2].

Taking $r = 1$ in Theorem 1 we get the following statement.

Corollary 1. For any $\varepsilon > 0$ there is a positive effective constant $c(\varepsilon)$ with the following property. Let $\mathbb{F}/\mathbb{Q}$ be a Galois extension of degree D. Then for any $\alpha \in \mathbb{F}^*$ which is not a root of unity we have

$$h(\alpha) \geq c(\varepsilon) D^{-1/2-\varepsilon} .$$

For a direct proof of this corollary, which uses [2] instead of the deeper result of [4], see [6] exercise 16.23, which was the starting point of our investigation.

We remark that Corollary 1 is optimal: take for $\mathbb{F}$ the splitting field of $x^d - 2$, with $D = d\phi(d)$, and $\alpha = 2^{1/d}$. Nevertheless, as mentioned above, this result can be strengthened for a *generator* α of a Galois extension.

Theorem 2. For any $\varepsilon > 0$ there is a positive effective constant $c(\varepsilon)$ with the following property. Let $\alpha \in \overline{\mathbb{Q}}^*$ be of degree d, not a root of unity, such that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois. Then we have

$$h(\alpha) \geq c(\varepsilon) d^{-\varepsilon} .$$

Again, the proof builds on the method of [1] and on the Relative Dobrowolki Theorem of [2].

References

[1] F. Amoroso and S. David, "Le problème de Lehmer en dimension supérieure", *J. Reine Angew. Math.* **513** (1999), 145–179.

[2] F. Amoroso and U. Zannier, "A relative Dobrowolski's lower bound over abelian extensions." *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **29** (2000), no. 3, 711–727.

[1] which implies that α is not a root of unity.

[3] P. Borwein, E. Dobrowolski and M. Mossinghoff. "Lehmer's problem for polynomials with odd coefficients". *Bull. London Math. Soc.*, **36**, 332–338 (2004).
[4] E. Delsinne, "Le problème de Lehmer relatif en dimension supérieure", *Ann. Sci. École Norm. Sup.* **42**, fascicule 6 (2009), 981–1028.
[5] E. Dobrowolski, "On a question of Lehmer and the number of irreducible factors of a polynomial". *Acta Arith.*, **34** (1979), 391–401.
[6] D. Masser, "Auxiliary Polynomials in Number Theory". In Press.
[7] M. Mignotte. "Estimations élémentaires effectives sur les nombres algébriques". *Publications I. R. M. A., Strasbourg*, (1979).
[8] C. J. Smyth, "On the product of the conjugates outside the unit circle of an algebraic number", *Bull. London Math. Soc.* **3** (1971), 169–175.

Reporter: Fabien Pazuki

Participants

Prof. Dr. Boris Adamczewski
Institut de Mathématiques de Marseille
Aix-Marseille Université, CMI
39, rue F. Joliot-Curie
13453 Marseille Cedex 13
FRANCE

Dr. Shabnam Akhtari
Department of Mathematics
University of Oregon
Eugene, OR 97403-1222
UNITED STATES

Prof. Dr. Francesco Amoroso
Laboratoire de Mathématiques Nicolas Oresme
Université de Caen
14032 Caen Cedex
FRANCE

Dr. Dzmitry Badziahin
Department of Mathematical Sciences
Durham University
Science Laboratories
South Road
Durham DH1 3LE
UNITED KINGDOM

Prof. Dr. Jason P. Bell
Department of Pure Mathematics
University of Waterloo
Waterloo, Ont. N2L 3G1
CANADA

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
Heslington, York Y010 5DD
UNITED KINGDOM

Prof. Dr. Daniel Bertrand
Institut de Mathématiques
Université Pierre et Marie Curie
Tour 46, 5eme etage
4, Place Jussieu
75252 Paris Cedex 05
FRANCE

Prof. Dr. Yuri Bilu
A2X, IMB
Université Bordeaux
351, cours de la Libération
33405 Talence Cedex
FRANCE

Prof. Dr. Yann Bugeaud
I R M A
Université de Strasbourg
7, rue René Descartes
67084 Strasbourg Cedex
FRANCE

Prof. Dr. Nicolas Chevallier
Laboratoire de Mathématiques
Université de Haute Alsace
4, rue des Frères Lumière
68093 Mulhouse Cedex
FRANCE

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

Prof. Dr. Eric Delaygue
Institut Camille Jordan
Université Claude Bernard Lyon 1
43 blvd. du 11 novembre 1918
69622 Villeurbanne Cedex
FRANCE

Dr. Jan-Hendrik Evertse
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
NETHERLANDS

Prof. Dr. Clemens Fuchs
Fachbereich Mathematik
Universität Salzburg
Hellbrunnerstrasse 34
5020 Salzburg
AUSTRIA

Dr. Ziyang Gao
Institut de Mathématiques de Jussieu
Bat. Sophie Germain
5, rue Thomas Mann
75205 Paris Cedex 13
FRANCE

Prof. Dr. Eric Gaudron
Laboratoire de Mathématiques
UMR 6620 du CNRS
Université Blaise Pascal-Clermont II
Plateau des Cezeaux
63177 Aubière Cedex
FRANCE

Prof. Dr. Philipp Habegger
Mathematisches Institut
Universität Basel
Spiegelgasse 1
4051 Basel
SWITZERLAND

Dr. Alan Haynes
Department of Mathematics
University of York
Heslington, York YO10 5DD
UNITED KINGDOM

Prof. Dr. Marc Hindry
U. F. R. de Mathématiques
Université Paris VII
Case 7012
2, Place Jussieu
75251 Paris Cedex 05
FRANCE

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

Prof. Dr. Patrick Ingram
Department of Mathematics
Colorado State University
Weber Building
Fort Collins, CO 80523-1874
UNITED STATES

Dr. Dijana Kreso
Institut für Mathematik
Technische Universität Graz
Steyrergasse 30
8010 Graz
AUSTRIA

Dr. Holly Krieger
Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
UNITED STATES

Dr. Lars Kühne
Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
GERMANY

Prof. Dr. Michel Laurent
Institut de Mathématiques de Marseille
Case 907
163 Avenue de Luminy
13288 Marseille Cedex 9
FRANCE

Prof. Dr. Aaron D. Levin
Department of Mathematics
Michigan State University
East Lansing, MI 48824-1027
UNITED STATES

Prof. Dr. Elon Lindenstrauss
Einstein Institute of Mathematics
The Hebrew University
Givat Ram
91904 Jerusalem
ISRAEL

Dr. Davide Lombardo
Laboratoire de Mathématiques
Université Paris Sud (Paris XI)
Batiment 425
91405 Orsay Cedex
FRANCE

Antoine Marnat
Institut für Analysis und Zahlentheorie
Technische Universität Graz
Steyrergasse 30
8010 Graz
AUSTRIA

Dr. Guillaume Maurin
Institut de Mathématiques de Jussieu
Theorie des Nombres, Case 247
Université de Paris VI
4, Place Jussieu
75252 Paris Cedex 05
FRANCE

Prof. Dr. Nikolay G. Moshchevitin
Department of Mechanics &
Mathematics
Moscow State University
ul. Leninskiye Gory, 1
119 992 Moscow
RUSSIAN FEDERATION

Prof. Dr. Yuri V. Nesterenko
Department of Mechanics &
Mathematics
Moscow Lomonosov State University
Vorobjovy Gory
119 899 Moscow
RUSSIAN FEDERATION

Prof. Dr. Fabien Pazuki
Department of Mathematical Sciences
University of Copenhagen
Universitetsparken 5
2100 Copenhagen
DENMARK

Prof. Dr. Patrice Philippon
Institut de Mathématiques de Jussieu
Théorie des Nombres
Université de Paris VI
4, Place Jussieu
75252 Paris Cedex 05
FRANCE

Dr. Lukas Pottmeyer
Mathematisches Institut
Universität Basel
Spiegelgasse 1
4051 Basel
SWITZERLAND

Prof. Dr. Gaël Rémond
Institut Fourier
UMR 5582, CNRS/UGA
Université Grenoble Alpes
100, rue des maths
38402 Saint-Martin-d'Hères Cedex
FRANCE

Prof. Dr. Tanguy Rivoal
Laboratoire de Mathématiques
Institut Fourier
Université de Grenoble I
BP 74
38402 Saint-Martin-d'Heres Cedex
FRANCE

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

Dr. Harry Schmidt
Mathematical Institute
Oxford University
24-29 St. Giles
Oxford OX1 3LB
UNITED KINGDOM

Prof. Dr. Joseph H. Silverman
Department of Mathematics
Brown University
Box 1917
Providence, RI 02912
UNITED STATES

Prof. Dr. Thomas Tucker
Department of Mathematics
University of Rochester
Rochester, NY 14627
UNITED STATES

Peter Varju
Centre for Mathematical Sciences
University of Cambridge
Wilberforce Road
Cambridge CB3 0WB
UNITED KINGDOM

Dr. Sanju Velani
Department of Mathematics
University of York
Heslington, York YO10 5DD
UNITED KINGDOM

Prof. Dr. Carlo Viola
Dipartimento di Matematica
"L. Tonelli"
Universita di Pisa
Largo Bruno Pontecorvo, 5
56127 Pisa
ITALY

Prof. Dr. Michel Waldschmidt
Institut de Mathématiques de Jussieu
Theorie des Nombres, Case 247
Université de Paris VI
4, Place Jussieu
75252 Paris Cedex 05
FRANCE

Dr. Martin Widmer
Department of Mathematics
Royal Holloway College
University of London
Surrey TW20 0EX
UNITED KINGDOM

Prof. Dr. Umberto Zannier
Fac. of Mathematics & Natural Sciences
Scuola Normale Superiore
Piazza dei Cavalieri, 7
56126 Pisa
ITALY

Prof. Dr. Michael Zieve
Department of Mathematics
University of Michigan
530 Church Street
Ann Arbor, MI 48109-1043
UNITED STATES

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

Prof. Dr. Evgeniy Zorin
Department of Mathematics
University of York
Heslington, York YO10 5DD
UNITED KINGDOM