Algebraic Dynamics and Transcendental Numbers

Michel Waldschmidt[1]

Institut de Mathématiques de Jussieu, Université P. et M. Curie, Théorie des Nombres, Case 247, 4, Place Jussieu, F-75252 PARIS Cedex 05 France

Abstract. A first example of a connection between transcendental numbers and complex dynamics is the following. Let p and q be polynomials with complex coefficients of the same degree. A classical result of Böttcher states that p and q are locally conjugates in a neighborhood of ∞: there exists a function f, conformal in a neighborhood of infinity, such that $f(p(z)) = q(f(z))$. Under suitable assumptions, f is a transcendental function which takes transcendental values at algebraic points. A consequence is that the conformal map (Douady-Hubbard) from the exterior of the Mandelbrot set onto the exterior of the unit disk takes transcendental values at algebraic points. The underlying transcendence method deals with the values of solutions of certain functional equations.

A quite different interplay between diophantine approximation and algebraic dynamics arises from the interpretation of the height of algebraic numbers in terms of the entropy of algebraic dynamical systems.

Finally we say a few words on the work of J.H. Silverman on diophantine geometry and canonical heights including arithmetic properties of the Hénon map.

1 Transcendental Values of Böttcher Functions

For any complex number $c \in \mathbf{C}$, define the polynomial $p_c \in \mathbf{C}[z]$ by $p_c(z) = z^2 + c$. For $n \geq 1$, let p_c^n be the n-th iterate of p_c:

$$p_c^1(z) = p_c(z) = z^2 + c, \qquad p_c^2(z) = p_c(z^2 + c) = (z^2 + c)^2 + c,$$

$$p_c^n(z) = p_c^{n-1}(z^2 + c) \qquad (n \geq 2).$$

The *Mandelbrot set* M can be defined as

$$M = \bigl\{c \in \mathbf{C} \mid p_c^n(0) \text{ does not tend to } \infty \text{ as } n \to \infty\bigr\}.$$

In 1982, A. Douady and J. Hubbard have shown that M is connected. They constructed a conformal map

$$\Phi : \mathbf{C} \setminus M \longrightarrow \{z \in \mathbf{C}\,;\, |z| > 1\}$$

from the complement of M onto the exterior of the unit disk, which is defined as follows.

For each $c \in \mathbf{C}$, there is a unique power series φ_c with coefficients in $\mathbf{Q}(c)$,

$$\varphi_c(z) = z + c_0 + \frac{c_1}{z} + \frac{c_2}{z^2} + \ldots \in \mathbf{Q}(c)((1/z)),$$

such that

$$\varphi_c(z^2 + c) = \varphi_c(z)^2.$$

For $c \notin M$, φ_c defines an analytic function near c. Then the above mentioned map Φ is defined by $\Phi(c) = \varphi_c(c)$.

According to P.G. Becker, W. Bergweiler and K. Nishioka [2], [3], [11], *for any algebraic* $\alpha \in \mathbf{C} \setminus M$*, the number* $\Phi(\alpha)$ *is transcendental.* .

The function φ_c is the unique *Böttcher function* with respect to $p_c = z^2 + c$ and z^2. More generally, let

$$p = az^d + \cdots \quad \text{and} \quad q = bz^d + \cdots$$

be two polynomials in $\mathbf{C}[z]$ of degree $d \geq 2$ and let $\lambda \in \mathbf{C}$ satisfy $\lambda^{d-1} = a/b$. There exists a unique function f, which is defined and meromorphic in a neighborhood of ∞, such that

$$\lim_{z \to \infty} \frac{f(z)}{\lambda z} = 1 \quad \text{and} \quad f\big(p(z)\big) = q\big(f(z)\big)$$

for sufficiently large $|z|$. Such a conjugating function f is called a *Böttcher function with respect to* p *and* q*.*

Assume p and q have algebraic coefficients and are not linearly conjugate to monomials or Chebychev polynomials. Then f *is a transcendental function, which takes transcendental values at algebraic points.*

This result holds more generally for classes of analytic functions which satisfy certain functional equations. There are two methods to study the transcendence of values of such functions.

The first one originates in the solution, by Th. Schneider, of Hilbert's seventh problem on the value of the exponential function, which satisfies the functional equation $f(z_1 + z_2) = f(z_1)f(z_2)$. This method can be used to consider other functional equations, like

$$f(z^d) = af(z)^d + bz^h.$$

The second method has been introduced by K. Mahler (see [11]) and enables one to prove transcendence results for the values of analytic functions f which are solutions of more general functional equations, like

$$P\big(z, f(z), f(z^d)\big) = 0.$$

In the present situation, both methods provide the desired result.

2 Lehmer's Problem and the Entropy of Algebraic Dynamical Systems

Let $F \in \mathbf{Z}[X]$ be a monic polynomial of degree $d \geq 1$ with complex roots $\alpha_1, \ldots, \alpha_d$. Define, for any positive integer n,

$$\Delta_n(F) = \prod_{i=1}^{d} (\alpha_i^n - 1) \in \mathbf{Z}.$$

In case $F = X - 2$ we have $\Delta_n(F) = 2^n - 1$, and the prime values of the sequence $2^n - 1$ are the so-called Mersenne primes. In 1933 [7], D.H. Lehmer suggested that the sequence $\Delta_n(F)$ is likely to produce prime numbers, provided that it grows slowly. If no $|\alpha_i|$ is 1, then

$$\lim_{n\to\infty} \frac{\Delta_{n+1}(F)}{\Delta_n(F)} = \prod_{\substack{1\leq i\leq n \\ |\alpha_i|>1}} |\alpha_i|.$$

More generally, for a polynomial

$$F = a_0 X^d + \cdots + a_d = a_0 \prod_{i=1}^{d} (X - \alpha_i) \in \mathbf{C}[X],$$

define, with K. Mahler,

$$M(F) = |a_0| \prod_{\substack{1\leq i\leq n \\ |\alpha_i|>1}} |\alpha_i| = \exp \int_0^1 \log |F(e^{2i\pi t})| dt.$$

For any polynomial $F \in \mathbf{C}[X]$, we have $M(F) \geq 1$. When $F \in \mathbf{Z}[X]$, we have $M(F) = 1$ if and only all its roots α_i are either zero or roots of unity. For his calculations, Lehmer used the polynomial $F(X) = X^3 - X - 1$. It turns out that this actually is the polynomial having smaller measure > 1 among the non reciprocal polynomials (its root > 1 is the smallest Pisot-Vijiyaraghavan number). For reciprocal polynomials F, that is for F satisfying $F(X^d) = X^d F(1/X)$, Lehmer said he could not find a polynomial having smaller measure than $M(F_0) = 1.1762808183\ldots$, with

$$F_0(X) = X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1 = X^5 Q\bigl(X + (1/X)\bigr)$$

and

$$Q(T) = (T+1)^2 (T-1)(T+2)(T-2) - 1.$$

He asked whether for each $c > 1$ there is a polynomial $F \in \mathbf{Z}[X]$ for which $1 < M(F) \leq c$, and this open question is known as *Lehmer's problem.*

The number $M(F)$ has a dynamical interpretation, which is a bridge between the notion of height of a polynomial and ergodic theory [6], [12], [5].

For our purposes, an algebraic dynamical system is a continuous endomorphism $T : X \to X$ of a metrizable compact topological group. The easiest case, which will be sufficient for our purpose, is the torus $X = \mathbf{T}^d = \mathbf{R}^d/\mathbf{Z}^d$. Each continuous endomorphism of $\mathbf{T}^d$ is given by a $d \times d$ matrix A_T with integer coefficients, and

$$T\mathbf{x} \equiv A_T\mathbf{x} \pmod 1.$$

Automorphisms are given by a matrix A_T with determinant 1 of -1.

An endomorphism T is "ergodic" if, whenever a measurable subset B of X (for a Haar measure μ) satisfies $T^{-1}B = B$, we have $\mu(B) = 0$ or 1. In the torus case $\mathbf{T}^d$, this condition amounts to say that for every square integrable function f, the condition $f(Tx) = f(x)$ almost everywhere implies that f is constant almost everywhere.

It follows that an endomorphism T is ergodic is and only if no eigenvalue of A_T is a root of unity. So we shall be interested in polynomials (namely the characteristic polynomial $\chi(A_T)$ of A_T) with no root a root of unity.

The set of periodic points of period n under T is

$$\mathrm{Per}_n(T) = \{x \in \mathbf{T}^d \mid T^n(x) = x\}.$$

If T is ergodic, then the number of periodic points of period n is

$$|\mathrm{Per}_n(T)| = |\det(A_T^n - I)| = |\Delta_n(\chi(A_T))|.$$

The *topological entropy* of T can be defined in terms of the metric: for $\epsilon > 0$ denote by B_ϵ the ball around the origin with radius ϵ. Then

$$h(T) = \lim_{\epsilon\to 0}\lim_{n\to\infty} -\frac{1}{n}\log\mu\left(\cap_{j=0}^{n-1}T^{-j}(B_\epsilon)\right).$$

Denote by $\lambda_1, \ldots, \lambda_d$ the eigenvalues of A_T (counting multiplicities). Then Yuzvinskii's formula reads

$$h(T) = \sum_{i=1}^{d}\log\max\{1, |\lambda_i|\}.$$

Hence the entropy of T is nothing else than the logarithm of Mahler's measure of the characteristic polynomial $\chi(A_T)$ of A_T.

Since any monic polynomial $X^d + a_1X^{d-1} + \cdots + a_d$ is the characteristic polynomial of a matrix, namely

$$A = \begin{pmatrix} 0 & & & \\ \vdots & & I_{d-1} & \\ 0 & & & \\ -a_d & -a_{d-1} & \cdots & -a_1 \end{pmatrix},$$

it follows that Lehmer's problem is equivalent to asking: *which values in* $[0, \infty]$ *can occur as an entropy?*

According to D.A. Lind, a positive answer to Lehmer's problem (i.e. the existence of polynomials in $\mathbf{Z}[X]$ with arbitrarily small $M(F) > 1$) is equivalent to the existence of a continuous endomorphism of the infinite torus $\mathbf{T}^{\mathbf{Z}}$ with finite entropy.

Interesting problems occur when one tries to replace the torus $\mathbf{R}/\mathbf{Z}$ by an elliptic curve [1].

This section has been prepared with the help of Paola D'Ambros.

3 Canonical Heights and Dynamical Systems

Define the *absolute multiplicative height* of a polynomial $F \in \mathbf{Z}[X]$ of degree $d > 0$ by

$$H(F) = M(F)^{1/d}$$

and the *absolute multiplicative height* of an algebraic number α by

$$H(\alpha) = H(F)$$

where $F \in \mathbf{Z}[X]$ is the minimal polynomial of α over $\mathbf{Z}$. The name is motivated by the property

$$H(\alpha^n) = H(\alpha)^n$$

for any algebraic number α and any positive integer n. Hence this height H behaves nicely with respect to the polynomials $\phi(X) = X^n$.

J.H. Silverman [18] introduced a height function which behaves nicely for an arbitrary rational function ϕ with algebraic coefficients, viewed as a map $\mathbf{P}_1(\overline{\mathbf{Q}}) \rightarrow \mathbf{P}_1(\overline{\mathbf{Q}})$.

Definition. Let $\phi \in \overline{\mathbf{Q}}(X)$ be a rational function of degree $n \geq 2$. The *ϕ-canonical height* of an algebraic number is

$$\hat{H}_\phi(\alpha) = \lim_{r \to \infty} \bigl(\phi^r(\alpha)\bigr)^{1/n^r}, \qquad (*)$$

where $\phi^r = \phi \circ \phi^{r-1}$ and ϕ^0 is the identity.

This construction has been introduced by Tate in his work on Abelian varieties, and has been extended to this general context by Silverman in a series of papers. He proved:

The limit $(*)$ *defining* $\hat{H}_\phi(\alpha)$ *exists, and*

$$\hat{H}_\phi(\phi\alpha) = \hat{H}_\phi(\alpha)^n.$$

Moreover

$$\hat{H}_\phi(\alpha) \geq 1$$

for any $\alpha \in \overline{\mathbf{Q}}$*, with equality if and only if* α *is* pre-periodic for ϕ.

Recall that α is a *pre-periodic point for* ϕ if the orbit $\{\alpha, \phi\alpha, \phi^2\alpha, \ldots\}$ contains only finitely many points.

The natural generalization of Lehmer's conjecture to this more general setting had been raised by P. Moussa, J-S. Geronimo and D. Bessis in 1984 [10].

The rational map

$$\phi(X) = \frac{(X^2-1)^2}{4X^3+4X}$$

corresponds to the duplication map on the elliptic curve $Y^2 = X^3 + X$. For this map, and more generally for the rational maps corresponding to multiplication by an integer on an elliptic curve, partial results towards this Lehmer-type conjecture are known (M. Laurent, D.W. Masser and S.W. Zhang, M. Hindry and J. Silverman).

Variants of this construction have been proposed, mainly by J.H. Silverman. In [13], he defined heights on $K3$ surfaces using two involutions which generate an infinite group of automorphisms. With G.S. Call in [4], he did the same on general varieties V by using a morphism $\phi : V \to V$ and a divisor D for which $\phi^* D$ is linearly equivalent to αD with $\alpha > 1$. In [14], he considered a variety V related with the Hénon map

$$\phi : \mathbf{A}^2 \to \mathbf{A}^2, \qquad \phi(X,Y) = (Y, Y^2 + aX + b)$$

as follows: blowing up each of the points $(1:0:0)$ and $(0:1:0)$ three times, one obtains a variety V so that both ϕ and ϕ^{-1} extend to morphisms $V \to \mathbf{P}^2$. For $P \in \mathbf{A}^2(\overline{\mathbf{Q}})$, the relation

$$h(\phi^n P) + h(\phi^{-n} P) \geq (2^n + 2^{-n})\big(h(P) - c\big) + 2c$$

holds with some constant $c = c(\phi)$. Silverman used this inequality to prove that ϕ has only finitely many periodic points with rational coordinates and to count the growth rate of points in an infinite orbit.

The author wishes to thank Michel Planat for the excellent organization of this conference.

References

1. D'Ambros, P., Everest, G., Miles, R., Ward, T. (1999) Dynamical systems arising from elliptic curves. Manuscript, 9 pp.
2. Becker, P-G., Bergweiler, W. (1993) Transcendency of local conjugacies in complex dynamics and transcendency of their values. Manuscripta Math. **81** no. 3-4, 329–337.
3. Becker, P-G., Bergweiler, W. (1995) Hypertranscendency of conjugacies in complex dynamics. Math. Ann. **301** no. 3, 463–468.

4. Call, G. S., Silverman, J. H. (1993) Canonical heights on varieties with morphisms. Compositio Math. **89** no. 2, 163–205.
5. Everest, G., Ward, T. (1999) Heights of Polynomials and Entropy in Algebraic Dynamics. Springer, London.
6. Halmos, P. (1956) Lectures on ergodic theory. Publications of the Mathematical Society of Japan, no. 3, The Mathematical Society of Japan. Chelsea Publishing Co., New York 1960.
7. Lehmer, D.H. (1933) Factorization of certain cyclotomic functions. Ann. of Math. **34** 461–479.
8. Morton, P., Silverman, J. H. (1994) Rational periodic points of rational functions. Internat. Math. Res. Notices no. 2, 97–110.
9. Morton, P., Silverman, J. H. (1995) Periodic points, multiplicities, and dynamical units. J. Reine Angew. Math. **461**, 81–122.
10. Moussa, P., Geronimo, J. S., Bessis, D. (1984) Ensembles de Julia et propriétés de localisation des familles itérées d'entiers algébriques. C. R. Acad. Sci. Paris Sér. I Math. **299** no. 8, 281–284.
11. Nishioka, Kumiko (1996) Mahler functions and transcendence. Lecture Notes in Mathematics **1631**, Springer-Verlag, Berlin.
12. Schmidt, K. (1995) Dynamical systems of algebraic origin. Birkhäuser, Progress in Math. **128**.
13. Silverman, J. H. (1991) Rational points on $K3$ surfaces: a new canonical height. Invent. Math. **105**, no. 2, 347–373.
14. Silverman, J. H. (1993) Integer points, Diophantine approximation, and iteration of rational maps. Duke Math. J. **71** no. 3, 793–829.
15. Silverman, J. H. (1994) Geometric and arithmetic properties of the Hénon map. Math. Z. **215** no. 2, 237–250.
16. Silverman, J. H. (1995) The field of definition for dynamical systems on $\mathbf{P}^1$. Compositio Math. **98** no. 3, 269–304.
17. Silverman, J. H. (1996) Rational functions with a polynomial iterate. J. Algebra **180** no. 1, 102–110.
18. Silverman, J. H. (1996) Small Salem numbers, exceptional units, and Lehmer's conjecture. Symposium on Diophantine Problems (Boulder, CO, 1994). Rocky Mountain J. Math. **26** no. 3, 1099–1114.