

Simultaneous rational approximation to exponentials of algebraic numbers

Damien Roy

University of Ottawa

Diophantine Approximation and Homogeneous Dynamics

University of York (by Zoom), September 23, 2020

- *Simultaneous approximation to values of the exponential function over the adeles, Mathematische Annalen* **377(3)** (2020), 1057–1093.
- *French and English versions available on arXiv.*

Part I: A first observation

$$e^z = \sum_{k=0}^{\infty} \frac{z^k}{k!}$$

- for all $z \in \mathbb{C}$,
- for all $z \in \mathbb{C}_p$ with $|z|_p < p^{-1/(p-1)}$.

• Euler (1748):

$$e = [2, (1, 2n, 1)_{n=1}^{\infty}] = [2, 1, \mathbf{2}, 1, 1, \mathbf{4}, 1, \dots] = 2 + \frac{1}{1 + \frac{1}{\mathbf{2} + \frac{1}{1 + \dots}}}$$

◇ Similar continued fraction expansions for e^r with $r \in \mathbb{Q} \setminus \{0\}$

when $r = \frac{2}{m}$ for some $m \in \mathbb{Z} \setminus \{0\}$ (Euler, Sundman, Hurwitz)

i.e. **whenever e^r makes sense only in $\mathbb{R}$.**

◇ No observed pattern otherwise. . . Why?

A further question

- $e = [2, (1, 2n, 1)_{n=1}^{\infty}] \Rightarrow \left| e - \frac{p}{q} \right| \geq \frac{\log \log(4q)}{18q^2 \log(4q)}$ (Bundshuh, 1971)
- Numerical experiments yield

$$\left| e^3 - \frac{p}{q} \right| \geq \frac{1}{3q^2 \log(q) \log \log(q)} \quad \text{if } 4 \leq q \leq 10^{500\,000}$$

- Let $r \in \mathbb{Q}$. Does there exist a constant g such that

$$\left| e^r - \frac{p}{q} \right| \geq \frac{1}{q^2 \log(q)^g} \quad \text{when } q \text{ is large enough?}$$

Interlude : The adelic Minkowski's convex body theorem

Let K be a number field, and let $d = [K : \mathbb{Q}]$.

A place v of K comes

- either from an embedding $\sigma: K \rightarrow \mathbb{C}$ (case $v|\infty$) – then set
 - ▶ $|x|_v := |\sigma(x)|$ ($x \in K$),
 - ▶ $d_v := [K_v : \mathbb{R}] = 1$ or 2 ,
 - ▶ $\mu_v =$ Lebesgue measure on K_v ,
- or from an embedding $\sigma: K \rightarrow \mathbb{C}_p$ (case $v|p$) – then set
 - ▶ $|x|_v = |\sigma(x)|_p$ ($x \in K$),
 - ▶ $d_v := [K_v : \mathbb{Q}_p]$,
 - ▶ $\mathcal{O}_v = \{x \in K_v; |x|_v \leq 1\}$,
 - ▶ $\mu_v =$ Haar measure on K_v with $\mu_v(\mathcal{O}_v) = 1$.

The field K embeds diagonally in $K_{\mathbb{A}} = \prod'_v K_v$ as a discrete subgroup with finite covolume with respect to $\mu = \prod_v \mu_v$.

An **adelic convex body** of K^s is a product $\mathcal{C} = \prod_v \mathcal{C}_v \subset K_{\mathbb{A}}^s$ such that

- (i) when $v \mid \infty$, then $\mathcal{C}_v$ is a compact convex neighborhood of 0 in K_v^s such that $\alpha \mathcal{C}_v = \mathcal{C}_v$ for any $\alpha \in K_v$ with $|\alpha|_v = 1$;
- (ii) if $v \nmid \infty$, then $\mathcal{C}_v$ is a finitely generated (thus free) sub- $\mathcal{O}_v$ -module of K_v^s of rank s ;
- (iii) $\mathcal{C}_v = \mathcal{O}_v^s$ for all but finitely many places v of K with $v \nmid \infty$.

Its **i -th minimum** $\lambda_i(\mathcal{C})$ is the smallest $\lambda > 0$ such that

$$\lambda \mathcal{C} := \prod_{v \mid \infty} \lambda \mathcal{C}_v \prod_{v \nmid \infty} \mathcal{C}_v$$

contains at least i linearly independent elements of K^s .

Theorem (McFeat 1971, Bombieri and Vaaler 1983, Thunder 2002)

$$\lambda_1(\mathcal{C})^d \cdots \lambda_s(\mathcal{C})^d \mu(\mathcal{C}) \asymp 1.$$

Example

Take $K = \mathbb{Q}$ and $\mathcal{C} = \mathcal{C}_\infty \times \prod_p \mathbb{Z}_p^s$.

- $\mu(\mathcal{C}) = \mu_\infty(\mathcal{C}_\infty)$,
- Given $\mathbf{x} \in \mathbb{Q}^s$, we find

$$\mathbf{x} \in \lambda \mathcal{C} = \lambda \mathcal{C}_\infty \times \prod_p \mathbb{Z}_p^s \iff \mathbf{x} \in \lambda \mathcal{C}_\infty \text{ and } \mathbf{x} \in \bigcap_p \mathbb{Z}_p^s = \mathbb{Z}^s$$

Thus $\lambda_i(\mathcal{C}) =$ standard i -th minimum of $\mathcal{C}_\infty$ with respect to $\mathbb{Z}^s$.

- We recover the usual Minkowski's theorem:

$$\lambda_1(\mathcal{C}_\infty) \cdots \lambda_s(\mathcal{C}_\infty) \mu_\infty(\mathcal{C}_\infty) \asymp 1.$$

Part II : Hermite's approximations

- **Hermite (1873):** $e \notin \bar{\mathbb{Q}}$
- **Lindemann (1882):** $\pi \notin \bar{\mathbb{Q}}$
- **Lindemann-Weierstrass theorem (Weierstrass, 1885):**

If $\alpha_1, \dots, \alpha_s \in \bar{\mathbb{Q}}$ are distinct, then $e^{\alpha_1}, \dots, e^{\alpha_s}$ are linearly independent over $\mathbb{Q}$.

Reformulation: Let $K \subset \mathbb{C}$ be a number field and let $\alpha_1, \dots, \alpha_s \in K$ be distinct. Then $e^{\alpha_1}, \dots, e^{\alpha_s}$ are linearly independent over K .

Proof:

- Choose a linear combination of $e^{\alpha_1}, \dots, e^{\alpha_s}$ over K .
- Take the product of its conjugates over $\mathbb{Q}$.
- Apply Hermite approximations to the exponential values.

Hermite's construction

Fix:

- K a number field,
- $\alpha_1, \dots, \alpha_s \in K$ distinct,
- $\mathbf{n} = (n_1, \dots, n_s) \in \mathbb{Z}_{>0}^s$.

Set:

- $f_{\mathbf{n}}(z) = (z - \alpha_1)^{n_1} \cdots (z - \alpha_s)^{n_s} \in K[z],$
- $P_{\mathbf{n}}(z) = \sum_{k=0}^N f_{\mathbf{n}}^{(k)}(z)$ where $N = \sum n_k = \deg(f_{\mathbf{n}}),$
- $a_{\mathbf{n}} := (P_{\mathbf{n}}(\alpha_1), \dots, P_{\mathbf{n}}(\alpha_s)) \in K^s.$

Then $a_{\mathbf{n}}$ is a “good approximation” to $(e^{\alpha_1}, \dots, e^{\alpha_s}).$

Rough estimates

Recall that $K \subset \mathbb{C}$ and $P_n(z) = \sum_{k=0}^N f_n^{(k)}(z) = \sum_{k=0}^{\infty} f_n^{(k)}(z)$, so

$$\frac{d}{dz}(P_n(z)e^{-z}) = (P_n'(z) - P_n(z))e^{-z} = -f_n(z)e^{-z}$$

$$\bullet \left| P_n(\alpha_i)e^{-\alpha_i} - P_n(\alpha_j)e^{-\alpha_j} \right| = \left| \int_{\alpha_i}^{\alpha_j} f_n(z)e^{-z} dz \right| \ll R^N$$

where $R = \max |\alpha_i - \alpha_j|$.

$$\bullet \left| P_n(\alpha_i) \right| = \left| \int_{\alpha_i}^{\infty} f_n(z)e^{-z} dz \right| \ll N!$$

$$\bullet P_n(\alpha_i) \in (n_i!)\mathcal{O}_K \text{ if } \alpha_1, \dots, \alpha_s \in \mathcal{O}_K.$$

A non-zero determinant

Let $\mathbf{e}_1 = (1, 0, \dots, 0), \dots, \mathbf{e}_s = (0, \dots, 0, 1)$.

Theorem (Mahler (1931))

Suppose that $\mathbf{n} = (n_1, \dots, n_s) \in \mathbb{Z}_{>0}^s$. Then $a_{\mathbf{n}-\mathbf{e}_1}, \dots, a_{\mathbf{n}-\mathbf{e}_s} \in K^s$ are linearly independent with

$$\Delta_{\mathbf{n}} := \det(a_{\mathbf{n}-\mathbf{e}_1}, \dots, a_{\mathbf{n}-\mathbf{e}_s}) = \prod_{i=1}^s \left((n_i - 1)! \prod_{k \neq i} (\alpha_i - \alpha_k)^{n_k} \right) \neq 0.$$

Main result (outline)

We construct a natural adelic convex body in terms of the values of $e^{\alpha_i - \alpha_j}$ in all completions K_v of K where they make sense, and show that the points $a_{\mathbf{n}-\mathbf{e}_1}, \dots, a_{\mathbf{n}-\mathbf{e}_s}$ realize its successive minima up to a factor $N^{\mathcal{O}(1)}$.

Archimedean components

For each $v \mid \infty$ associated to an embedding $\sigma: K \hookrightarrow \mathbb{C}$, define $R_v = \max |\alpha_i - \alpha_j|_v$ and

$$\mathcal{C}_{\mathbf{n},v} : \begin{cases} |x_i|_v \leq e^{R_v}(N-1)! \\ |x_i e^{\alpha_j - \alpha_i} - x_j|_v \leq \max_{1 \leq k \leq s} \left| \int_{\sigma(\alpha_i)}^{\sigma(\alpha_j)} f_{\mathbf{n} - \mathbf{e}_k}^{\sigma}(z) e^{\sigma(\alpha_j) - z} dz \right| \end{cases}$$

Then $a_{\mathbf{n} - \mathbf{e}_1}, \dots, a_{\mathbf{n} - \mathbf{e}_s} \in \mathcal{C}_{\mathbf{n},v}$ and $\mu_v(\mathcal{C}_{\mathbf{n},v}) = N^{\mathcal{O}(1)} |\Delta_{\mathbf{n}}|_v^{d_v}$.

Ultrametric components

Let $v \mid p$. If $|\alpha_i - \alpha_j|_v \neq 1$ for at least one choice of $i \neq j$ define

$$\mathcal{C}_{\mathbf{n},v} : \begin{cases} |x_i|_v \leq p^3 N \prod_{1 \leq k \leq s} \max \{ |\alpha_i - \alpha_k|_v, p^{-1/(p-1)} \}^{n_k} \\ |x_i e^{\alpha_j - \alpha_i} - x_j|_v \leq^{(*)} p^3 N \prod_{1 \leq k \leq s} \max \{ |\alpha_i - \alpha_k|_v, |\alpha_j - \alpha_k|_v \}^{n_k} \end{cases}$$

(*) whenever $0 < |\alpha_j - \alpha_i|_v < p^{-1/(p-1)}$. Otherwise set

$$\mathcal{C}_{\mathbf{n},v} := (n_1 - 1)! \mathcal{O}_v \times \cdots \times (n_s - 1)! \mathcal{O}_v.$$

Then $a_{\mathbf{n}-\mathbf{e}_1}, \dots, a_{\mathbf{n}-\mathbf{e}_s} \in \mathcal{C}_{\mathbf{n},v}$ and $\mu_v(\mathcal{C}_{\mathbf{n},v}) = N^{\mathcal{O}(1)} |\Delta_{\mathbf{n}}|_v^{d_v}$.

More precisely, we have $\mu_v(\mathcal{C}_{\mathbf{n},v}) = |\Delta_{\mathbf{n}}|_v^{d_v}$ in the second case.

Main result

Set $\mathcal{C}_{\mathbf{n}} = \prod_v \mathcal{C}_{\mathbf{n},v}$. Then,

- (i) $\mathbf{a}_{\mathbf{n}-\mathbf{e}_1}, \dots, \mathbf{a}_{\mathbf{n}-\mathbf{e}_s} \in \mathcal{C}_{\mathbf{n}}$,
- (ii) $\mu(\mathcal{C}_{\mathbf{n}}) = N^{\mathcal{O}(1)}$,
- (iii) $\lambda_i(\mathcal{C}_{\mathbf{n}}) = N^{\mathcal{O}(1)}$ for $i = 1, \dots, s$.

Proof.

(i) is clear,

(ii) $\mu(\mathcal{C}_{\mathbf{n}}) = \prod_v \mu_v(\mathcal{C}_{\mathbf{n},v}) = N^{\mathcal{O}(1)} \prod_v |\Delta_{\mathbf{n}}|_v^{d_v} = N^{\mathcal{O}(1)},$

(iii) We have $\lambda_1(\mathcal{C}_{\mathbf{n}}) \leq \dots \leq \lambda_s(\mathcal{C}_{\mathbf{n}}) \leq 1$ and, by the adelic Minkowski's theorem, $\prod_{i=1}^s \lambda_i(\mathcal{C}_{\mathbf{n}})^d \asymp \mu(\mathcal{C}_{\mathbf{n}})^{-1} = N^{\mathcal{O}(1)}.$



Corollary 1. Suppose that $K = \mathbb{Q}$ or that K is imaginary quadratic, and that $\alpha \in K$ has $|\alpha|_v \geq p^{-1/(p-1)}$ whenever $v \mid p$. Then, there exists $c > 0$ such that

$$|x| |xe^\alpha - y| \geq (\log |x|)^{-c}$$

for each $x, y \in \mathcal{O}_K$ with $|x|$ large enough.

Examples:

- $K = \mathbb{Q}(\sqrt{-2})$ and $\alpha = 2(1 \pm \sqrt{-2})/m$ with $m \in \mathcal{O}_K \setminus \{0\}$,
- $K = \mathbb{Q}(\sqrt{-23})$ and $\alpha = (1 \pm \sqrt{-23})/(2m)$ with $m \in \mathcal{O}_K \setminus \{0\}$.

Corollary 2. The convex body $\mathcal{C}_\infty$ of $\mathbb{R}^2$ defined by

$$\mathcal{C}_\infty : \begin{cases} |x| \leq \frac{(2n)!}{n!3^{n/2}}, \\ |xe^3 - y|_v \leq \left(\frac{3}{2}\right)^{2n} \frac{1}{n!3^{n/2}} \end{cases}$$

has minima $n^{\mathcal{O}(1)}$ with respect to the lattice

$$\Lambda = \{(x, y) \in \mathbb{Z}^2; |xe^3 - y|_3 \leq 3^{-n}\}.$$

$\Rightarrow \quad |x| |xe^3 - y| \geq |x|^{-c/\log \log |x|}$ for all $x, y \in \mathbb{Z}$ with $|x|$ large enough.

Conjecture. There exists a constant $c > 0$ such that

$$|x|_\infty |xe^3 - y|_\infty |x|_3 |xe^3 - y|_3 \geq (\log |x|)^{-c}$$

for all $x, y \in \mathbb{Z}$ with $|x|$ large enough.

Part III: Paths of steepest descent

Fix $\alpha_1, \dots, \alpha_s \in \mathbb{C}$ distinct. Set

$$f(z) = (z - \alpha_1)^{n_1} \cdots (z - \alpha_s)^{n_s}$$

with $n_1, \dots, n_s \in \mathbb{Z}_{>0}$.

Problem: Estimate $\left| \int_{\alpha_i}^{\alpha_j} f(z) e^{-z} dz \right|$ from above.

- Choose a path $\gamma: [0, 1] \rightarrow \mathbb{C}$ such that $\gamma(0) = \alpha_i$, $\gamma(1) = \alpha_j$. Then

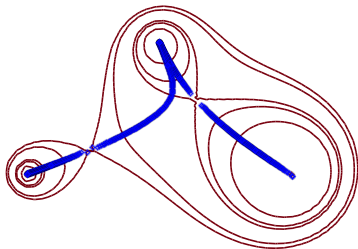
$$\left| \int_{\alpha_i}^{\alpha_j} f(z) e^{-z} dz \right| \leq \mathcal{L}(\gamma) \cdot \boxed{\max_{\gamma} |f|} \cdot \max_{\gamma} |e^{-z}|.$$

$\uparrow$
(length)

$\uparrow$
want this as small as possible

- Consider the level curves $|f| = r$ as r increases.

Example : $f(z) = z(z - 1)^2(z - (1 + i)/2)$ ($s = 3$)



- They meet at zeros of $f'(z)/f(z)$.

- **Goal:** Compose paths of steepest descent for $|f|$ from those points

Parametrization

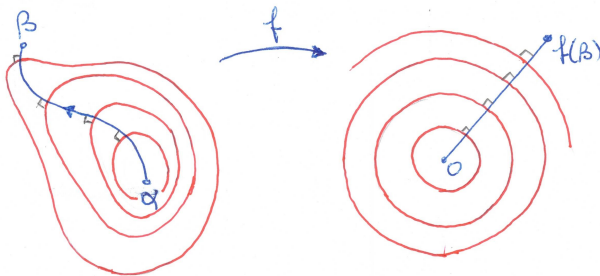
Fix β in the convex hull $\mathcal{K}$ of $A = \{\alpha_1, \dots, \alpha_s\}$.

A path of steepest descent for $|f|$ from β ends in a root $\alpha \in A$ of f .

(i) It can be parametrized (at reverse) by a continuous piece-wise differentiable function $\gamma: [0, 1] \rightarrow \mathbb{C}$ such that $\gamma(0) = \alpha$, $\gamma(1) = \beta$ and

$$f(\gamma(t)) = tf(\beta) \quad (0 \leq t \leq 1).$$

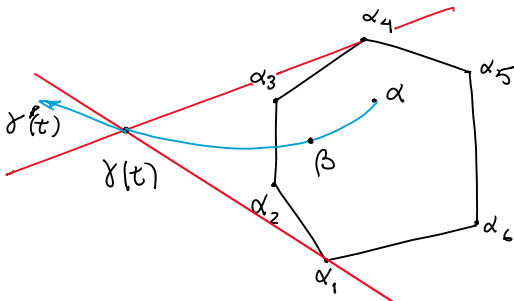
Proof. The map $f: \mathbb{C} \rightarrow \mathbb{C}$ is conformal outside on the set of roots of f' and maps level curves of $|f|$ to circles centered at 0.



$$(ii) \quad \gamma([0, 1]) \subseteq \mathcal{K}$$

Proof. Since $f(\gamma(t)) = tf(\beta)$, we have

$$\gamma'(t) = \frac{f(\beta)}{f'(\gamma(t))} = \frac{f(\gamma(t))}{tf'(\gamma(t))} = \frac{1}{t} \left(\sum_{j=1}^s \frac{n_j}{\gamma(t) - \alpha_j} \right)^{-1}.$$



The path does not come back to $\mathcal{K}$.

$$(iii) \quad \mathcal{L}(\gamma) \leq \pi NR \text{ where } N = \sum n_i = \deg(f) \text{ and } R = \max |\alpha_i|.$$

Proof. Cauchy-Crofton formula gives:

$$\mathcal{L}(\gamma) = \frac{1}{4} \int_0^{2\pi} d\theta \int_{-R}^R N(r, \theta) dr$$

where $N(r, \theta) = \#\{t \in [0, 1]; \gamma(t) \in D_{r, \theta}\}$

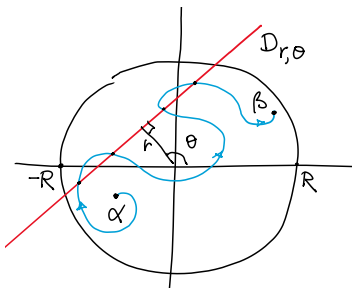
and $D_{r, \theta} = \{(r + iu)e^{i\theta}; u \in \mathbb{R}\}.$

Since $f(\gamma(t))/f(\beta) = t \in \mathbb{R}$ for $t \in [0, 1]$, we find

$$N(r, \theta) \leq \#\left\{u \in \mathbb{R}; \operatorname{Im} \frac{f((r + iu)e^{i\theta})}{f(\beta)} = 0\right\} \leq N$$

except for at most N angles $\theta \in [0, 2\pi).$

Problem: Is $\mathcal{L}(\gamma)$ bounded from above independently of $(n_1, \dots, n_s)$?
(I can show: $\mathcal{L}(\gamma) \leq \pi sR$ if $\alpha \in \partial\mathcal{K}.$)



A tree of paths

Write

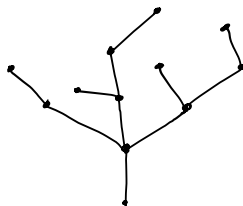
$$f'(z) = N(z - \alpha_1)^{n_1-1} \cdots (z - \alpha_s)^{n_s-1} (z - \beta_1)^{m_1} \cdots (z - \beta_p)^{m_p}$$

Then $\sum m_k = s - 1$ and we have

$$B := \{\beta_1, \dots, \beta_p\} \subset \mathcal{K} \quad \text{by Gauss-Lucas theorem.}$$

A *tree* is a connected graph with **no cycle**

$$\begin{array}{c} \Updownarrow \\ |\text{edges}| = |\text{vertices}| - 1 \end{array}$$



Theorem

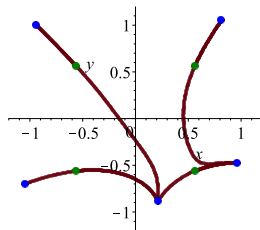
There is a tree such that

- (i) *its vertices are $\alpha_1, \dots, \alpha_s$,*
- (ii) *each edge is labelled by β_k for some $k = 1, \dots, p$,*
- (iii) *there are m_k edges labelled by β_k for $k = 1, \dots, p$,*
- (iv) *if an edge $\{\alpha_i, \alpha_j\}$ is labelled by β_k , there is a path $\gamma: [0, 1] \rightarrow \mathbb{C}$ of length at most $2\pi RN$, contained in $\mathcal{K}$, such that $\gamma(0) = \alpha_i$, $\gamma(1/2) = \beta_k$, $\gamma(1) = \alpha_j$ and*

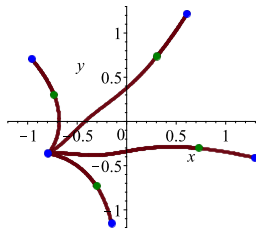
$$\max_{0 \leq t \leq 1} |f(\gamma(t))| = |f(\beta_k)|.$$

$$(iv) \implies \left| \int_{\alpha_i}^{\alpha_j} f(z) e^{-z} dz \right| \leq (2\pi NR) |f(\beta_k)| e^R.$$

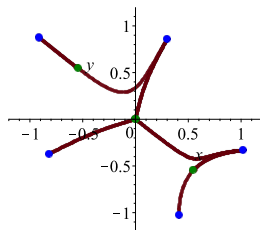
Examples



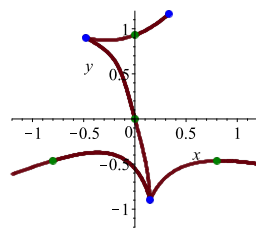
The tree for $z^5 + 2z + 2i - 1$.



The tree for $z^5 + 2iz + 2i - 1$.



The tree for $z^5 + iz^3 - 1 + 0.7i$.



The tree for $z^5 + 2iz^2 + 2i - 1$.

Thank you!

