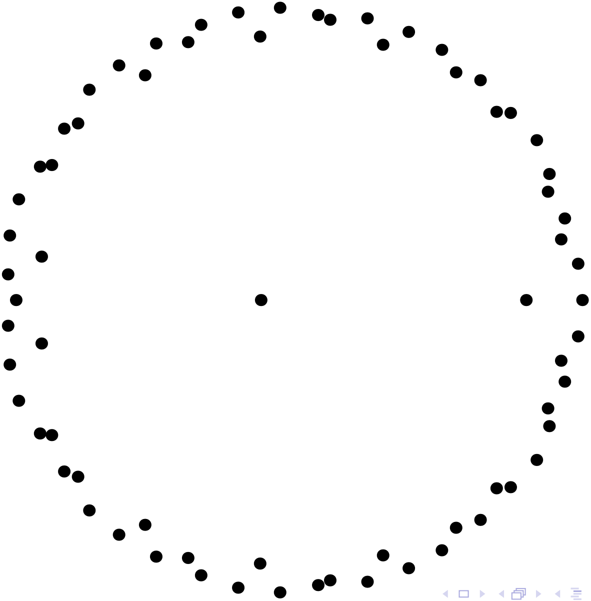
The method of asymptotic expansions of Poincaré and Mahler measures of univariate polynomials in the Conjecture of Lehmer

Jean-Louis Verger-Gaugry

CNRS
LAMA, Université Savoie Mont Blanc,
Institut Fourier, Université Grenoble Alpes,
France

BIRS
The Geometry, Algebra and Analysis of Algebraic Numbers
Oct 4 - Oct 9, 2015

Contents



N bodies in space ("N-body problem")

1895
(Poincaré)

Equation
(Newton)

N bodies in space ("N-body problem")

1895

(Poincaré)

Equation

(Newton)

N bodies in space ("N-body problem")

1895

(Poincaré)

Equation

(Newton)

N bodies in space ("N-body problem")

1895
(Poincaré)

Equation
(Newton)

1895 : Henri Poincaré, *Leçons de Mécanique Céleste*,
Paris Gauthier-Villars,

t. I (1905), *Théorie générale des perturbations planétaires*,
t. II-1 (1907), *Développement de la fonction perturbatrice*,
t. II-2 (1909), *Théorie de la Lune*,
t. III (1910), *Théorie des marées*.

gives courses at the Sorbonne, Paris.

Theory of Asymptotic expansions (Copson, Erdelyi, Dingle...)

Divergent series (Hardy),

Divergent sums of functions of time

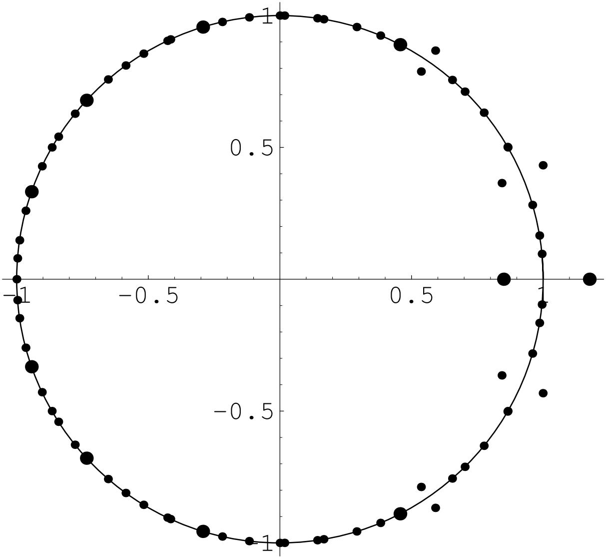
-> relative position of EACH planet at time $t + \delta t$, once given at time t : as an asymptotic expansion of time t.

Theory of Asymptotic expansions (Copson, Erdelyi, Dingle...)

Divergent series (Hardy),

Divergent sums of functions of time

-> relative position of EACH planet at time $t + \delta t$, once given at time t : as an asymptotic expansion of time t.


1
0.5
-1
-0.5
0.5
1
-0.5
-1

N zeroes z_i in $\mathbb{C}$ (“close to $|z| = 1$")

Cj Lehmer

small Mahler measure

$< 1.32\ldots$

Equation

(polynomial eq., rec. monic)

(having the z_is as zeroes)

N zeroes z_i in $\mathbb{C}$ ("close to $|z| = 1$")

Cj Lehmer

small Mahler measure

$< 1.32\ldots$

Equation

(polynomial eq., rec. monic)

(having the z_is as zeroes)

N zeroes z_i in $\mathbb{C}$ (“close to $|z| = 1$")

Cj Lehmer

small Mahler measure

$< 1.32\ldots$

Equation

(polynomial eq., rec. monic)

(having the z_is as zeroes)

N zeroes z_i in $\mathbb{C}$ ("close to $|z| = 1$")

Cj Lehmer
small Mahler measure
$< 1.32\ldots$

Equation
(polynomial eq., rec. monic)
(having the z_is as zeroes)

Is the method of asymptotic expansions of H. Poincaré applicable in this numbertheoretic context ?

how ? : trinomials $-1 + X + X^n$, $n \geq 2$ (VG 2015)

Each z_i becomes a function of ? analog of time t ?
The Mahler measure $\prod_{|z_i| \geq 1} |z_i|$ also.

$$\mathrm{M}(\alpha) = \sum_{q=0}^{r-1} a_q \varphi_q(n?) + O\left(\varphi_r(n?)\right) \qquad n? \to +\infty.$$

Is the method of asymptotic expansions of H. Poincaré applicable in this numbertheoretic context ?

how ? : trinomials $-1 + X + X^n, \quad n \geq 2$ (VG 2015)

Each z_i becomes a function of ? analog of time t ?
The Mahler measure $\prod_{|z_i|\geq 1} |z_i|$ also.

$$\mathrm{M}(\alpha) = \sum_{q=0}^{r-1} a_q \varphi_q(n?) + O\left(\varphi_r(n?)\right) \qquad n? \to +\infty.$$

Is the method of asymptotic expansions of H. Poincaré applicable in this numbertheoretic context ?

how ? : trinomials $-1 + X + X^n, \quad n \geq 2$ (VG 2015)

Each z_i becomes a function of ? analog of time t ? The Mahler measure $\prod_{|z_i| \geq 1} |z_i|$ also.

$$\mathrm{M}(\alpha) = \sum_{q=0}^{r-1} a_q \varphi_q(n?) + O\left(\varphi_r(n?)\right) \qquad n? \to +\infty.$$

Contents

Degree

?

Conjecture of Lehmer (1933) : in the search of big prime numbers, Lehmer asked the following problem : *if ϵ is a positive quantity, to find a polynomial of the form*

$$f(x) = x^r + a_1 x^{r-1} + \ldots + a_r$$

where the a's are integers, such that the absolute value of the product of those roots of f which lie outside the unit circle, lies between 1 *and* $1 + \epsilon$*... Whether or not the problem has a solution for* $\epsilon < 0.176$ *we do not know*.

Conjecture of Schinzel-Zassenhaus (1965) : $\alpha \neq 0$ any algebraic integer of degree n, not being a root of unity,

$$\overline{|\alpha|} \geq 1 + \frac{c_1}{n}$$

for a constant $c_1 > 0$ (i.e. independent of n).

Conjecture of Lehmer (1933) : in the search of big prime numbers, Lehmer asked the following problem : *if ϵ is a positive quantity, to find a polynomial of the form*

$$f(x) = x^r + a_1 x^{r-1} + \ldots + a_r$$

where the a's are integers, such that the absolute value of the product of those roots of f which lie outside the unit circle, lies between 1 *and* $1 + \epsilon$*... Whether or not the problem has a solution for* $\epsilon < 0.176$ *we do not know*.

Conjecture of Schinzel-Zassenhaus (1965) : $\alpha \neq 0$ any algebraic integer of degree n, not being a root of unity,

$$\lceil \alpha \rceil \geq 1 + \frac{c_1}{n}$$

for a constant $c_1 > 0$ (i.e. independent of n).

Dobrowolski (1979) :

$$\mathrm{M}(\alpha) \; > \; 1 + (1-\epsilon)\left(\frac{\mathrm{Log}\,\mathrm{Log}\, n}{\mathrm{Log}\, n}\right)^3, \quad n > n_1(\epsilon).$$

for any nonzero algebraic number α of degree n [Effective : replace $1-\epsilon$ by $1/1200$].

Voutier (1996) : same minoration with the constant

$$1/4$$

and all $n \geq 2$.

Dobrowolski (1979) :

$$\mathrm{M}(\alpha) \ > \ 1 + (1-\epsilon)\left(\frac{\mathrm{Log}\,\mathrm{Log}\, n}{\mathrm{Log}\, n}\right)^{3}, \quad n > n_1(\epsilon).$$

for any nonzero algebraic number α of degree n [Effective : replace $1-\epsilon$ by $1/1200$].

Voutier (1996) : same minoration with the constant

$$1/4$$

and all $n \geq 2$.

Kronecker (1857) : α an algebraic integer,

$$\overline{|\alpha|} = 1 \text{ if and only if } \alpha \text{ is a root of unity.}$$

The sufficient condition was weakened by **Blansky and Montgomery (1971)** who showed that α, with $\deg \alpha = n$, is a root of unity provided

$$\overline{|\alpha|} \leq 1 + \frac{1}{30n^2 \operatorname{Log}(6n)}.$$

Dobrowolsky (1978) sharpened this condition by : if

$$\overline{|\alpha|} < 1 + \frac{\operatorname{Log} n}{6n^2},$$

then α is a root of unity.

Kronecker (1857) : α an algebraic integer,

$$\overline{|\alpha|} = 1 \text{ if and only if } \alpha \text{ is a root of unity.}$$

The sufficient condition was weakened by **Blansky and Montgomery (1971)** who showed that α, with $\deg \alpha = n$, is a root of unity provided

$$\overline{|\alpha|} \leq 1 + \frac{1}{30n^2 \operatorname{Log}(6n)}.$$

Dobrowolsky (1978) sharpened this condition by : if

$$\overline{|\alpha|} < 1 + \frac{\operatorname{Log} n}{6n^2},$$

then α is a root of unity.

Kronecker (1857) : α an algebraic integer,

$$\overline{|\alpha|} = 1 \text{ if and only if } \alpha \text{ is a root of unity.}$$

The sufficient condition was weakened by **Blansky and Montgomery (1971)** who showed that α, with $\deg \alpha = n$, is a root of unity provided

$$\overline{|\alpha|} \leq 1 + \frac{1}{30n^2 \operatorname{Log}(6n)}.$$

Dobrowolsky (1978) sharpened this condition by : if

$$\overline{|\alpha|} < 1 + \frac{\operatorname{Log} n}{6n^2},$$

then α is a root of unity.

Laurent (1983) : techniques of transcendance theory. -> Elliptic curves, Abelian analog of Lehmer problem (Conjecture of Hindry (1997) for abelian varieties over a number field).

Interpolation determinants : Waldschmidt quoting : That *n* is closely related to the degree, but different in some cases, is common : quoting **Waldschmidt** (2000), "*we insist that n is only an upper bound for the degree of* α*, and not the actual degree*".

Perturbing polynomials :

⋮

G.A. Ray (1994)
M.J. Mossinghoff, C.G Pinner and J.D. Vaaler (1998)
E. Hironaka (2005)

⋮

Contents

n zeroes z_i in $\mathbb{C}$ (of the polynomial "$-1 + X + X^n$")

Equation

$-1 + z + z^y$

(y real variable, $y \geq 2$)

n zeroes z_i in $\mathbb{C}$ (of the polynomial "$-1 + X + X^n$")

Equation

$-1 + z + z^y$

(y real variable, $y \geq 2$)

n zeroes z_i in $\mathbb{C}$ (of the polynomial "$-1 + X + X^n$")

Equation

$-1 + z + z^y$

(y real variable, $y \geq 2$)

$$G_n(X) := -1 + X + X^n$$
$$G_n^*(X) = X^n G_n(1/X)$$

$\theta_n :=$ unique root of G_n in $(0,1)$
$\theta_n^{-1} :=$ dominant root of $G_n^*(X)$.
with (Selmer) :

$\theta_n^{-1} > 1$, is a Perron number,
$\lim_{n\to+\infty} \theta_n = \lim_{n\to+\infty} \theta_n^{-1} = 1$

For the family $\{\theta_n^{-1}\}$:
Solve : Conjectures of Lehmer, of Schinzel-Zassenhaus
improve : Voutier's minoration.
$(\mathrm{M}(G_n) = \mathrm{M}(G_n^*) = \mathrm{M}(\theta_n^{-1}) = \mathrm{M}(\theta_n))$

$$G_n(X) := -1 + X + X^n$$
$$G_n^*(X) = X^n G_n(1/X)$$

$\theta_n :=$ unique root of G_n in $(0, 1)$
$\theta_n^{-1} :=$ dominant root of $G_n^*(X)$.
with (Selmer) :

$\theta_n^{-1} > 1$, is a Perron number,
$\lim_{n \to +\infty} \theta_n = \lim_{n \to +\infty} \theta_n^{-1} = 1$

For the family $\{\theta_n^{-1}\}$:

Solve : Conjectures of Lehmer, of Schinzel-Zassenhaus
improve : Voutier's minoration.
$(\mathrm{M}(G_n) = \mathrm{M}(G_n^*) = \mathrm{M}(\theta_n^{-1}) = \mathrm{M}(\theta_n))$

$$G_n(X) := -1 + X + X^n$$
$$G_n^*(X) = X^n G_n(1/X)$$

$\theta_n :=$ unique root of G_n in $(0,1)$
$\theta_n^{-1} :=$ dominant root of $G_n^*(X)$.
with (Selmer) :

$\theta_n^{-1} > 1$, is a Perron number,
$\lim_{n\to+\infty} \theta_n = \lim_{n\to+\infty} \theta_n^{-1} = 1$

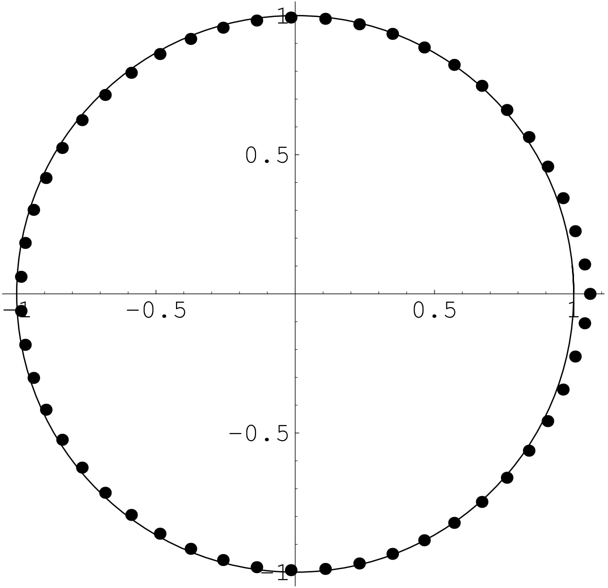
For the family $\{\theta_n^{-1}\}$:
Solve : Conjectures of Lehmer, of Schinzel-Zassenhaus
improve : Voutier's minoration.
$(\mathrm{M}(G_n) = \mathrm{M}(G_n^*) = \mathrm{M}(\theta_n^{-1}) = \mathrm{M}(\theta_n))$

$$G_n(X) := -1 + X + X^n$$
$$G_n^*(X) = X^n G_n(1/X)$$

$\theta_n :=$ unique root of G_n in $(0,1)$
$\theta_n^{-1} :=$ dominant root of $G_n^*(X)$.
with (Selmer) :

$\theta_n^{-1} > 1$, is a Perron number,
$\lim_{n\to+\infty} \theta_n = \lim_{n\to+\infty} \theta_n^{-1} = 1$

For the family $\{\theta_n^{-1}\}$:
Solve : Conjectures of Lehmer, of Schinzel-Zassenhaus
improve : Voutier's minoration.
$(\mathrm{M}(G_n) = \mathrm{M}(G_n^*) = \mathrm{M}(\theta_n^{-1}) = \mathrm{M}(\theta_n))$


1
0.5
-1
-0.5
0.5
1
-0.5
-1

Theorem (Smyth)

Let χ_3 be the uniquely specified odd character of conductor 3 ($\chi_3(m) = 0, 1$ or -1 according to whether $m \equiv 0$, 1 or 2 $\pmod 3$), equivalently $\chi_3(m) = \left(\frac{m}{3}\right)$ the Jacobi symbol), and denote $L(s, \chi_3) = \sum_{m \geq 1} \frac{\chi_3(m)}{m^s}$ the Dirichlet L-series for the character χ_3. Then

$$\begin{aligned}\lim_{n\to+\infty} \mathrm{M}(G_n) &= \exp\left(\frac{3\sqrt{3}}{4\pi}\mathrm{L}(2,\chi_3)\right)\\ &= \exp\left(\frac{-1}{\pi}\int_0^{\pi/3} \mathrm{Log}\left(2\sin\left(\frac{x}{2}\right)\right)dx\right)\\ &= 1.38135\ldots =: \Lambda.\end{aligned}$$

Theorem

Let n_0 be an integer such that $\frac{\pi}{3} > 2\pi \frac{\operatorname{Log} n_0}{n_0}$, and let $n \geq n_0$. Then,

$$\mathrm{M}(G_n) \;=\; \left(\lim_{m \to +\infty} \mathrm{M}(G_m)\right) \left(1 + r(n)\,\frac{1}{\operatorname{Log} n} + O\left(\frac{\operatorname{Log}\operatorname{Log} n}{\operatorname{Log} n}\right)^2\right)$$

with the constant $1/6$ involved in the Big O, and with $r(n)$ real, $|r(n)| \leq 1/6$.

$n = \deg \theta_n^{-1}$ if $n \not\equiv 5 \pmod 6$, and $n = \deg \theta_n^{-1} + 2$ if $n \equiv 5 \pmod 6$.

Corollary

$$\mathrm{M}(\theta_n^{-1}) \ > \ \Lambda - \frac{\Lambda}{6}\left(\frac{1}{\mathrm{Log}\, n}\right), \quad n \geq n_1 = 2.$$

Theorem

For all $n \geq 2$,

$$\boxed{\theta_n^{-1}} = \theta_n^{-1} \geq 1 + \frac{c}{n},$$

with $c = 2(\theta_2^{-1} - 1) = 1.2360\ldots$ reached only for $n = 2$, and,

$$\boxed{\theta_n^{-1}} = \theta_n^{-1} \;>\; 1 + \frac{(\mathrm{Log}\, n)\left(1 - \frac{\mathrm{Log}\,\mathrm{Log}\, n}{\mathrm{Log}\, n}\right)}{n}.$$

off extremality (Rhin, Wu). Here :
$n = \deg \theta_n^{-1}$ if $n \not\equiv 5 \pmod 6$, and $n = \deg \theta_n^{-1} + 2$ if $n \equiv 5 \pmod 6$.

Extremality

Denote by $\mathrm{m}(n)$ the minimum of the houses of the algebraic integers of degree n which are not a root of unity. An algebraic integer α, of degree n, is said *extremal* if $\lceil\overline{\alpha}\rceil = \mathrm{m}(n)$. An extremal algebraic integer is not necessarily a Perron number.

Conjecture (Lind - Boyd)

The smallest Perron number of degree $n \geq 2$ has minimal polynomial

$$\begin{array}{cl} X^n - X - 1 & \textit{if } \; n \not\equiv 3,5 \mod 6, \\ (X^{n+2} - X^4 - 1)/(X^2 - X + 1) & \textit{if } \; n \equiv 3 \mod 6, \\ (X^{n+2} - X^2 - 1)/(X^2 - X + 1) & \textit{if } \; n \equiv 5 \mod 6. \end{array}$$

Conjecture (Boyd)

(i) If α is extremal, then it is always nonreciprocal,
(ii) if $n = 3k$, then the extremal α has minimal polynomial

$$X^{3k} + X^{2k} - 1, \qquad \text{or} \quad X^{3k} - X^{2k} - 1,$$

(iii) the extremal α of degree n has asymptotically a number of conjugates $\alpha^{(i)}$ outside the closed unit disc equal to

$$\cong \frac{2}{3} n, \qquad n \to \infty.$$

Conjecture (Smyth)

For all integers $n \geq 4,\ k \geq 1$ *such that gcd*$(n, k) = 1,\ k < n/2$,

- $\mathrm{M}(z^n + z^k + 1) < \Lambda$ *if and only if 3 divides* $n + k$,
- $\mathrm{M}(z^n - z^k + 1) < \Lambda$ *with n odd if and only if 3 does not divide* $n + k$,
- $\mathrm{M}(z^n - z^k - 1) < \Lambda$ *with n even if and only if 3 does not divide* $n + k$.

Smyth's conjecture was recently proved by Flammang (2014) for large n.

Comparison : asymptotic expansions vs Smyth/Boyd/Duke's method :

Theorem

Let $n \geq 2$ be an integer. Then,

$$\mathrm{M}(-1+X+X^n) = \left(\lim_{m\to+\infty} \mathrm{M}(G_m)\right)\left(1+\frac{s(n)}{n^2}+O(n^{-3})\right)$$

with, for n odd :

$$s(n) = \begin{cases} \sqrt{3}\pi/18 = +0.3023\ldots & \text{if } n \equiv 1 \text{ or } 3 \pmod 6, \\ -\sqrt{3}\pi/6 = -0.9069\ldots & \text{if } n \equiv 5 \pmod 6, \end{cases}$$

for n even :

$$s(n) = \begin{cases} -\sqrt{3}\pi/36 = -0.1511\ldots & \text{if } n \equiv 0 \text{ or } 4 \pmod 6, \\ +\sqrt{3}\pi/12 = +0.4534\ldots & \text{if } n \equiv 2 \pmod 6. \end{cases}$$

Other trinomials

Conjecture :

$$\mathrm{M}(X^n + aX^k + b) > c_0 - c_2/\mathrm{Log}\, n$$

n ? - Strankov (2014), Flammang (2015).

VG : *On the Conjecture of Lehmer, limit Mahler measure of trinomials and asymptotic expansions*, UDT J. (2015).

Other trinomials

Conjecture :

$$\mathrm{M}(X^n + aX^k + b) > c_0 - c_2/\operatorname{Log} n$$

n ? - Strankov (2014), Flammang (2015).

VG : *On the Conjecture of Lehmer, limit Mahler measure of trinomials and asymptotic expansions*, UDT J. (2015).