In this lecture we consider the class of integer polynomials

$$\mathscr{C} := \{-1 + x + x^n + x^{m_1} + x^{m_2} + \ldots + x^{m_s} :$$

$$n \geq 3, m_1 - n \geq n-1, m_q - m_{q-1} \geq n-1 \quad \text{for} \quad 2 \leq q \leq s\}.$$

trinomial $-1 + x + x^n$ + a Newman polynomial

lacunarity : $n-1$

ex : $-1 + x + x^6, \;\; -1 + x + x^6 + x^{27} + x^{32},$
$1 + x + x^6 + x^{27} + x^{32} + x^{129} + x^{614}, \ldots$

class

$$\mathscr{C} := \{-1 + x + x^n + x^{m_1} + x^{m_2} + \ldots + x^{m_s} :$$
$$n \geq 3, m_1 - n \geq n - 1, m_q - m_{q-1} \geq n - 1 \quad \text{for} \quad 2 \leq q \leq s\}.$$

Main Obj : **zeroes, factorization**, as functions

- of $n$ (lacunarity) and $(m_1, \ldots, m_s)$,
- of the zeroes of $-1 + x + x^n$, when $n$ and $s$ become large, expressed as explicit functions of $n$, with :

$\rightarrow$ the study of the limit, $n$ fixed, for $s$ tending to $\infty$, and $n$ tending to infinity.

Goal : non-trivial **minoration of the Mahler measure** of real reciprocal algebraic integers, not roots of unity (Pb of Lehmer).

Lecture 4.I :

- class of lacunary polynomials,

- Problem of Lehmer, Mahler measure, Conjecture of Lehmer

- roots of $P \in \mathscr{C}$ - asymptotic expansions, the case of trinomials

- factorization - Ljunggren

ooooooo

Lecture 4.II : Rényi systems of numeration associated to $\mathscr{C}$, rewriting trails, a lenticular curve, universal minoration of the Mahler measure.

Definition : Weil height : let $\alpha \in \overline{\mathbb{Q}}^*$, $P_\alpha(X) = a_0(X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_n)$ $= a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n \in \mathbb{Z}[X],\ a_0 a_n \neq 0$, its minimal polynomial.

The (abs. log.) Weil height of $\alpha$ is

$$h(\alpha) = \frac{1}{n}\mathrm{Log}\left(|a_0| \prod_{i=1}^{n} \max\{1, |\alpha_i|\}\right)$$

Prop : $h(p/q) = \mathrm{Log}\max(|p|, |q|)$, $(p,q) = 1$, $\quad h(1) = 0$,
$h(\alpha) \geq 0$ for all $\alpha \in \overline{\mathbb{Q}}^*$,
$h(\alpha^r) = |r| h(\alpha)$, for $r \in \mathbb{Z}$, $\alpha \in \overline{\mathbb{Q}}^*$, $\quad h(1/\alpha) = h(\alpha)$,
$h(\sigma(\alpha)) = h(\alpha)$, for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Definition : Mahler measure : for

$$P(X) = a_0(X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_n) =$$
$$a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n \in \mathbb{Z}[X], \qquad a_0 a_n \neq 0$$

then

$$\mathrm{M}(P) := |a_0| \prod_{i, |\alpha_i| \geq 1} |\alpha_i|.$$

multiplicativity : $P = P_1 \times P_2 \times \ldots \times P_m, \Rightarrow \mathrm{M}(P) = \mathrm{M}(P_1) \ldots \mathrm{M}(P_m)$.

ex. : $P = \Phi_1 \times \ldots \times \Phi_r \times R$ with $R$ irr. pol., $\Phi_j$ cyclot. $\Longrightarrow \mathrm{M}(P) = \mathrm{M}(R)$.

$\alpha$ alg. number, deg $\alpha = n$, $P_\alpha$ his minimal polynomial, $\mathrm{M}(\alpha) := \mathrm{M}(P_\alpha)$.
Absolute logarithmic, Weil height of $\alpha$ :

$$h(\alpha) := \frac{\mathrm{Log}\,\mathrm{M}(\alpha)}{d}$$

facts : $\mathrm{M}(\alpha) = \mathrm{M}(\alpha^{-1})$,

$\mathrm{M}(\alpha) = \alpha$ if $\alpha \in$ S (= set of Pisot numbers ; $|\alpha_i| < 1$),

$\mathrm{M}(\alpha) = \alpha$ if $\alpha \in$ T (= set of Salem numbers ; $|\alpha_i| < 1$ with at least one $|\alpha_j| = 1$),

$\mathrm{M}(\alpha) = 1$ if $\alpha$ is a root of unity.

<u>Kronecker's Theorem</u>(1857) : Let $\alpha$ be a nonzero algebraic integer. Then $\mathrm{M}(\alpha) = 1$ iff $\alpha$ is a root of unity.

practice in Arithm. Geo. :

$\mathrm{M}(\alpha)$ calculated $\rightarrow$ useful to calculate $h(\alpha)$,

height $h$ = sum of local contributions $\rightarrow$ useful to prove Theorems.

Adler Marcus (1979) (topological entropy and equivalence of dynamical systems), Perron-Frobenius theory) :

$$\{\mathrm{M}(\alpha) \mid \alpha \text{ alg. number}\} \subset \mathbb{P}_{Perron},$$

$$\{\mathrm{M}(P) \mid P \in \mathbb{Z}[X]\} \subset \mathbb{P}_{Perron}.$$

Two strict inclusions (Dubickas 2004, Boyd 1981).

Definition : $\alpha \in \mathbb{P}_{Perron}$ if $\alpha = 1$ or if $\alpha > 1$ is a real algebraic integer, for which the conjugates $\alpha^{(i)}$ satisfy $|\alpha^{(i)}| < \alpha$ (i.e. dominant root $> 1$).

Northcott's Theorem : for all $B \geq 0$, $d \geq 1$,

$$\#\{\alpha \in \overline{\mathbb{Q}} \mid h(\alpha) \leq B, [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq d\} < +\infty.$$

in Dio. Geom. : bound on "degree" + bound on "$h$" gives finiteness property (Mordell eff., etc).

**Conjecture of Lehmer : there exists $c > 0$ such that**

$$\mathrm{M}(\alpha) \geq 1 + c$$

**for any algebraic number $\alpha \neq 0$ which is not a root of unity,**

i.e. the interval $(1, 1 + c) \cap \mathbb{P}_{Perron}$ is deprived of any value of Mahler measure of any algebraic number.

$->$ values : discontinuity at 1 (meaning, sense, of $c$ ?).

# Lehmer's problem (1933)

in the exhaustive search for large prime numbers : *if $\varepsilon$ 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 $a_i$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* $1+\varepsilon$*... Whether or not the problem has a solution for* $\varepsilon < 0.176$ *we do not know*.

Lehmer's strategy : $P_\alpha$ with small $\mathrm{M}$ : useful to obtain large prime numbers $p$, in the Pierce numbers of $\alpha$. Iwasawa theory : large powers of primes. Einsiedler, Everest and Ward : study of the density of such $p$s.

## Lehmer's Problem is a limit problem + restrictions :

$$\mathrm{M}(P) := |a_0| \prod_{i, |\alpha_i| \geq 1} |\alpha_i| \quad \Longrightarrow \quad \mathrm{M}(P) := |a_0| \geq |a_0|.$$

Let $\alpha \in \overline{\mathbb{Q}}, \; P = P_\alpha$ :

- $*$ if $\alpha \in \overline{\mathbb{Q}} \setminus \mathscr{O}_{\overline{\mathbb{Q}}}$ , then $|a_0| \geq 2 \quad \Longrightarrow \quad \mathrm{M}(P) \geq 2$,
- $*$ if $\alpha$ is an algebraic integer which is not reciprocal ($P_\alpha \neq P^*_\alpha$ with

$$P^*_\alpha(X) = X^{\deg P_\alpha} P_\alpha(1/X) \quad ),$$

Smyth's Theorem '71 $\Longrightarrow \mathrm{M}(P_\alpha) \geq \Theta = 1.32\ldots$ (= smallest Pisot number, $X^3 - X - 1$ mini. pol.).

## Lehmer's Problem is a limit problem for reciprocal algebraic integers :

$|\alpha| \neq 1$

$$\mathrm{M}(\alpha) := |\alpha| \prod_{i, |\alpha_i| \geq 1} |\alpha_i| \quad \Longrightarrow \quad \mathrm{M}(\alpha) \geq |\alpha|.$$

Lehmer's problem corresponds to an accumulation of conjugates, when the house $\overline{|\alpha|}$ tends to $1^+$.

The investigation has to bear only on the set of nonzero reciprocal algebraic integers which are not roots of unity.

## Roots of any $P \in \mathscr{C}$

Exact expressions of the roots of any $P(x) \in \mathscr{C}$ (then of their moduli, then of M).

what can be expected from “classical” theories ?

- Galois Theory : radical expressions (multiplication, addition, subtraction, division, extraction of roots, only permitted on the coefficients), in degrees $n \leq 6$, $m_s \leq 6$,

- Mellin Theory (1915) : hypergeometric multiple integrals - several variables, Mellin’s Inversion formula.

$$\gamma(y) = y^n + x_1 y^{n_1} + x_2 y^{n_2} + \ldots + x_p y^{n_p} - 1 = 0, \quad n > n_s \geq 1\,(s = 1, 2, \ldots, p)$$

The solution $y = y(x_1, x_2, \ldots, x_p)$ which takes the value 1 for $x_1 = x_2 = \ldots = x_p = 0$ is called

Mellin's *Hauptlösung*, or Principal Solution.

The other solutions are all obtained from it : if $\varepsilon^n = 1$, then

$$\varepsilon y(\varepsilon^{n_1} x_1, \varepsilon^{n_2} x_2, \ldots, \varepsilon^{n_p} x_p)$$

since :

$$(\varepsilon y)^n + (\varepsilon)^{-n_1} x_1 (\varepsilon y)^{n_1} + (\varepsilon)^{-n_2} x_2 (\varepsilon y)^{n_2} + \ldots + (\varepsilon)^{-n_p} x_p (\varepsilon y)^{n_p} - 1 = 0.$$

Mellin's parameters :

$$y = W^{-\frac{1}{n}}, \qquad W = 1 + \xi_1 + \xi_2 + \ldots + \xi_p$$

$$x_s = \xi_s W^{\frac{n_s}{n} - 1}$$

$$\frac{\partial(x_1, x_2, \ldots, x_p)}{\partial(\xi_1, \xi_2, \ldots, \xi_p)} = \left(1 + \frac{n_1}{n}\xi_1 + \frac{n_2}{n}\xi_2 + \ldots + \frac{n_p}{n}\xi_p\right) W^{\frac{n_1+n_2+\ldots+n_p}{n} - p - 1}$$

Then, for $\mu > 0$ large enough,

$$\int_0^\infty \int_0^\infty \ldots \int_0^\infty y^\mu x_1^{u_1 - 1} x_2^{u_2 - 1} \ldots x_p^{u_p - 1} dx_1 dx_2 \ldots dx_p$$

$$= \int_0^\infty \int_0^\infty \ldots \int_0^\infty y^\mu x_1^{u_1 - 1} x_2^{u_2 - 1} \ldots x_p^{u_p - 1} \frac{\partial(x_1, x_2, \ldots, x_p)}{\partial(\xi_1, \xi_2, \ldots, \xi_p)} d\xi_1 d\xi_2 \ldots d\xi_p$$

with $\Re(u_1) > 0, \Re(u_2) > 0, \ldots, \Re(u_p) > 0$, $\Re(\mu - n_1 u_1 - \ldots - n_p u_p) > 0$

Let $u = \frac{1}{n}(\mu - n_1 u_1 - \ldots - n_p u_p)$.

Then

$$= \int_0^\infty \int_0^\infty \ldots \int_0^\infty \Phi \ \times \xi_1^{u_1 - 1} \xi_2^{u_2 - 1} \ldots \xi_p^{u_p - 1} d\xi_1 d\xi_2 \ldots d\xi_p$$

with

$$\Phi = \frac{\left(1 + \frac{n_1}{n}\xi_1 + \frac{n_2}{n}\xi_2 + \ldots + \frac{n_p}{n}\xi_p\right)}{W^{u+u_1+u_2+\ldots+u_p+1}}.$$

now, use Mellin's inversion formula.

## Inversion Formula :

$$\int_0^\infty \int_0^\infty \dots \int_0^\infty \frac{1}{W^w} \xi_1^{u_1-1} \xi_2^{u_2-1} \dots \xi_p^{u_p-1} d\xi_1 d\xi_2 \dots d\xi_p$$

$$= \frac{\Gamma(u_1)\Gamma(u_2)\dots\Gamma(u_p)\Gamma(w-u_1-u_2\dots-u_p)}{\Gamma(w)}$$

## Principal solutions :

$(y(x_1, x_2, \ldots, x_p))^{\mu} =$

$$\left(\frac{1}{2i\pi}\right)^p \times \int_{a_1-i\infty}^{a_1+i\infty} \int_{a_2-i\infty}^{a_2+i\infty} \cdots \int_{a_p-i\infty}^{a_p+i\infty} F\, x_1^{-u_1} x_2^{-u_2} \ldots x_p^{-u_p} du_1 du_2 \ldots du_p$$

with

$$F = \frac{\mu}{n} \frac{\Gamma(u)\Gamma(u_1)\Gamma(u_2)\ldots\Gamma(u_p)}{\Gamma(u+u_1+u_2+\ldots+u_p+1)}$$

$$a_i > 0 \quad \text{well chosen}$$

and conditions of convergence.

Class $\mathscr{C}$ : coefficients $x_i$ in $\{0,1\}$ and lacunarity for

$$\gamma(y) = y^n + x_1 y^{n_1} + x_2 y^{n_2} + \ldots + x_p y^{n_p} - 1 = 0$$

(Mellin) the roots of a general algebraic equation can be expressed as hypergeometric multiple integrals bearing on the $\Gamma$-function.

Disadvantage :

- unsuitable to study the limit $n$ fixed and $s$ tending to infinity for $P \in \mathscr{C}$,
- does not take into account the factorization of any $P \in \mathscr{C}$,
- if $P(x) = -1 + x + x^n + Q(x) \in \mathscr{C}$ unable to establish the closeness of a subcollection of roots with the roots of $-1 + x + x^n$.

## Exact expressions of the roots of $-1+x+x^n$ as asymptotic expansions

Copson, Erdelyi, Dingle : Theory of asymptotic expansions. Given as D + tl, though ideally exact with infinitely many terms. Denote $\theta_n \in (0,1)$ the unique root of $G_n(x) := -1+x+x^n$, $n \geq 3$.

### Proposition

*Let $n \geq 3$. The root $\theta_n$ can be expressed as : $\theta_n = \mathrm{D}(\theta_n) + \mathrm{tl}(\theta_n)$ with* $\mathrm{D}(\theta_n) = 1 -$

$$\frac{\mathrm{Log}\, n}{n}\left(1 - \left(\frac{n - \mathrm{Log}\, n}{n\mathrm{Log}\, n + n - \mathrm{Log}\, n}\right)\left(\mathrm{Log}\,\mathrm{Log}\, n - n\mathrm{Log}\left(1 - \frac{\mathrm{Log}\, n}{n}\right) - \mathrm{Log}\, n\right)\right) \tag{1}$$

*and*

$$\mathrm{tl}(\theta_n) \;=\; \frac{1}{n} O\left(\left(\frac{\mathrm{Log}\,\mathrm{Log}\, n}{\mathrm{Log}\, n}\right)^2\right), \tag{2}$$

*with the constant $1/2$ involved in $O(\;)$.*

Proof : Let us put $\theta_n = 1 - \frac{t}{n}$ with $0 < t < n$. Then

$$\frac{t}{n} = (1 - \frac{t}{n})^n. \tag{3}$$

Let us show that $t < \operatorname{Log} n$. Let $g(x) = xe^x$ be the increasing function of the variable $x$ on $\mathbb{R}$. The equation (3) implies $\frac{t}{n} = (1 - \frac{t}{n})^n < e^{-t} \Leftrightarrow g(t) < n$. Since $n < n \operatorname{Log} n$ for $n \geq 3$ and $g(\operatorname{Log} n) = n \operatorname{Log} n$, we deduce the claim. Taking the logarithm of (3) we obtain

$$\operatorname{Log} t - \operatorname{Log} n \ = \ n \operatorname{Log}(1 - \frac{t}{n}) \ = \ -t - \frac{1}{2}\frac{t^2}{n} - \frac{1}{3}\frac{t^3}{n^2} - \ldots.$$

The identity

$$t + \operatorname{Log} t + \frac{1}{2}\frac{t^2}{n} + \frac{1}{3}\frac{t^3}{n^2} + \ldots \ = \ \operatorname{Log} n \tag{4}$$

has now to be inversed in order to obtain $t$ as a function of $n$.

For doing this, we put $t = \operatorname{Log} n + w$. Equation (4) transforms into the following equation in $w$ :

$$(\operatorname{Log} n + w) + \operatorname{Log}(\operatorname{Log} n + w) + \frac{1}{2}\frac{(\operatorname{Log} n + w)^2}{n} + \frac{1}{3}\frac{(\operatorname{Log} n + w)^3}{n^2} + \ldots = \operatorname{Log} n.$$

We deduce

$$w + \operatorname{Log}(\operatorname{Log} n) + \operatorname{Log}(1 + \frac{w}{\operatorname{Log} n}) + \frac{1}{2}\frac{\operatorname{Log}^2 n}{n}\left(1 + \frac{w}{\operatorname{Log} n}\right)^2$$
$$+ \frac{1}{3}\frac{\operatorname{Log}^3}{n^2}\left(1 + \frac{w}{\operatorname{Log} n}\right)^3 + \ldots \ = \ 0.$$

Since

$$n\operatorname{Log}(1 - \frac{\operatorname{Log} n}{n}) + \operatorname{Log} n = -\frac{1}{2}\frac{\operatorname{Log}^2 n}{n} - \frac{1}{3}\frac{\operatorname{Log}^3 n}{n^2} - \ldots$$

and that

$$\operatorname{Log}(1 + \frac{w}{\operatorname{Log} n}) = \frac{w}{\operatorname{Log} n} - \frac{w^2}{2\operatorname{Log}^2 n} + \frac{w^3}{3\operatorname{Log}^3 n} - \ldots$$

we have :

$$\operatorname{Log}\operatorname{Log} n - n\operatorname{Log}(1 - \frac{\operatorname{Log} n}{n}) - \operatorname{Log} n$$

$$= w\left[-1 - \frac{1}{\operatorname{Log} n} - \frac{\operatorname{Log} n}{n} - \frac{\operatorname{Log}^2 n}{n^2} - \frac{\operatorname{Log}^3 n}{n^3} - \ldots\right]$$

$$+ w^2\left[\frac{1}{2\operatorname{Log}^2 n} - \frac{1}{2n} - \frac{\operatorname{Log} n}{n^2} - \frac{6}{4}\frac{\operatorname{Log}^2 n}{n^3} - \ldots\right] + \ldots . \qquad (5)$$

The coefficient coeff($w$) of $w$ is

$$-1-\frac{1}{\operatorname{Log} n}-\frac{\operatorname{Log} n}{n}\left(1+\frac{\operatorname{Log} n}{n}+\left(\frac{\operatorname{Log} n}{n}\right)^{2}+\ldots\right)=\frac{-n\operatorname{Log} n-n+\operatorname{Log} n}{(\operatorname{Log} n)\,(n-\operatorname{Log} n)}.$$

We deduce

$$w=\frac{(\operatorname{Log} n)\,(n-\operatorname{Log} n)\,(\operatorname{Log}\operatorname{Log} n-n\operatorname{Log}(1-\frac{\operatorname{Log} n}{n})-\operatorname{Log} n)}{-n\operatorname{Log} n-n+\operatorname{Log} n}+\ldots, \qquad (6)$$

which gives the expression of $\mathrm{D}(\theta_n)$.
Let us write $w$ in (6) as $\mathrm{D}(w)+u$, where $u$ denotes the remaining terms.
Putting $w=\mathrm{D}(w)+u$ in (5) we obtain, for large $n$,

$$0 \;=\; u\,\mathrm{coeff}(w)+\mathrm{D}(w)^{2}\frac{1}{2\operatorname{Log}^{2} n}+\ldots.$$

Since, for large $n$, coeff($w$) $\cong -1$ and $\mathrm{D}(w)\cong -\operatorname{Log}\operatorname{Log} n$, we deduce :

$$u\cong\; O\left(\left(\frac{\operatorname{Log}\operatorname{Log} n}{\operatorname{Log} n}\right)^{2}\right),$$

with a constant $1/2$ involved in $O(\ )$. We deduce the tail $\mathrm{tl}(\theta_n)$ of $\theta_n$.

## Roots enumerated by increasing argument : $j = 1, 2, 3, \ldots$ from the real axis

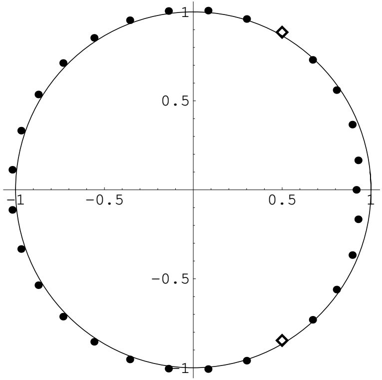


FIGURE: The roots (black bullets) of $G_n(x)$ (represented here with $n = 28$). A slight bump appears in the half-plane $\Re(z) > 1/2$ in the neighbourhood of 1, at the origin of the different regimes of asymptotic expansions.

$z_{j,n}$ roots : : obtain their asymptotic expansions, in a similar way.

a strictly increasing sequence with $j$ :

$$0 < \arg(z_{1,n}) < \arg(z_{2,n}) < \ldots < \arg(z_{\lfloor \frac{n}{2} \rfloor,n}) \leq \pi.$$

$$\text{angular sector to consider :}[-\pi/3, +\pi/3], \text{i.e.} \Re > 1/2.$$

We write

$$\theta_n = \mathrm{D}(\theta_n) + \mathrm{tl}(\theta_n),$$
$$\mathrm{Re}(z_{j,n}) = \mathrm{D}(\mathrm{Re}(z_{j,n})) + \mathrm{tl}(\mathrm{Re}(z_{j,n})),$$
$$\mathrm{Im}(z_{j,n}) = \mathrm{D}(\mathrm{Im}(z_{j,n})) + \mathrm{tl}(\mathrm{Im}(z_{j,n})),$$

where "D" stands for *"development"* (or *"limited expansion"*, or *"lowest order terms"*) and "tl" for *"tail"* (or "remainder", or *"terminant"*), and consider the products

$$\Pi_{G_n} := D(\mathrm{M}(G_n)) = D(\theta_n)^{-1} \times \prod_{z_{j,n} \text{ in } |z|<1, \Re>1/2} \mathrm{D}(|z_{j,n}|)^{-2}$$

instead of $\mathrm{M}(G_n)$, as approximant value of $\mathrm{M}(G_n)$.

**Theorem**

*Let $\chi_3$ 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 $\chi_3$. Then*

$$\lim_{n \to +\infty} \mathrm{M}(G_n) = \exp\left(\frac{3\sqrt{3}}{4\pi} \mathrm{L}(2, \chi_3)\right) = \exp\left(\frac{-1}{\pi} \int_0^{\pi/3} \mathrm{Log}\left(2 \sin\left(\frac{x}{2}\right)\right) dx\right)$$
$$= 1.38135\ldots =: \Lambda. \qquad (7)$$

**Theorem**

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

$$\mathrm{M}(-1+X+X^n) = \left(\lim_{m\to+\infty} \mathrm{M}(G_m)\right)\left(1+\frac{s(n)}{n^2}+O(n^{-3})\right) \qquad (8)$$

*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 :*

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

Why mod 6 ?

Theorem (Selmer)

*Let $n \geq 2$. If $n \not\equiv 5 \pmod 6$, then $G_n(X)$ is irreducible. If $n \equiv 5 \pmod 6$, then the polynomial $G_n(X)$ admits $X^2 - X + 1$ as irreducible factor in its factorization and $G_n(X)/(X^2 - X + 1)$ is irreducible.*

*In Lecture 4.II : we show that the class $\mathscr{C}$ "contains the solution" of the Problem of Lehmer, for $\alpha$ being* **real** $> 1$ *in the set of nonzero reciprocal algebraic integers (which are not roots of unity) :*

*by extending the method.*

Requirement in the general case : factorization of any $P \in \mathscr{C}$.

## Factorization and lacunarity of a $P \in \mathscr{C}$

In a series of papers, A. Schinzel had obtained general theorems on the factorization of lacunary polynomials into 3 components :

- cyclotomic part,
- reciprocal non-cyclotomic part,
- non-reciprocal part.

They are not sufficient to investigate the class $\mathscr{C}$, with the present objectives on the Mahler measure.

**Proposition**

*If $P(z) \in \mathbb{Z}[z]$, $P(1) \neq 0$, is nonreciprocal and irreducible, then $P(z)$ has no root of modulus $1$.*

Proof : Let $P(z) = a_d z^d + \ldots + a_1 z + a_0$, $a_0 a_d \neq 0$, be irreducible and nonreciprocal. We have $\gcd(a_0, \ldots, a_d) = 1$. If $P(\zeta) = 0$ for some $\zeta$, $|\zeta| = 1$, then $P(\overline{\zeta}) = 0$. But $\overline{\zeta} = 1/\zeta$ and then $P(z)$ would vanish at $1/\zeta$. Hence $P$ would be a multiple of the minimal polynomial $P^*$ of $1/\zeta$. Since $\deg(P) = \deg(P^*)$ there exists $\lambda \neq 0, \lambda \in \mathbb{Q}$, such that $P = \lambda P^*$.
In particular, looking at the dominant and constant terms, $a_0 = \lambda a_d$ and $a_d = \lambda a_0$. Hence, $a_0 = \lambda^2 a_0$, implying $\lambda = \pm 1$. Therefore $P^* = \pm P$. Since $P$ is assumed nonreciprocal, $P^* \neq P$, implying $P^* = -P$. Since $P^*(1) = P(1) = -P(1)$, we would have $P(1) = 0$. Contradiction.

## Study of the irreducibility of the nonreciprocal parts of the polynomials of $\mathscr{C}$ : method introduced by Ljunggren

**Lemma (Ljunggren)**

*Let $P(x) \in \mathbb{Z}[x]$, $\deg(P) \geq 2$, $P(0) \neq 0$. The nonreciprocal part of $P(x)$ is reducible if and only if there exists $w(x) \in \mathbb{Z}[x]$ different from $\pm P(x)$ and $\pm P^*(x)$ such that $w(x)\, w^*(x) = P(x)\, P^*(x)$.*

Proof : Let us assume that the nonreciprocal part of $P(x)$ is reducible. Then there exists two nonreciprocal polynomials $u(x)$ and $v(x)$ such that $P(x) = u(x)v(x)$. Let $w(x) = u(x)v^*(x)$. We have :

$$w(x)\, w^*(x) = u(x)v^*(x)u^*(x)v(x) = P(x)\, P^*(x).$$

Conversely, let us assume that the nonreciprocal part $c(x)$ of $P(x)$ is irreducible and that there exists $w(x)$ different of $\pm P(x)$ and $\pm P^*(x)$ such that $w(x)\,w^*(x) = P(x)\,P^*(x)$. Let $P(x) = a(x)c(x)$ be the factorization of $P$ where every irreducible factor in $a$ is reciprocal. Then

$$P(x)\,P^*(x) = a^2(x)\,c(x)\,c^*(x) = w(x)\,w^*(x).$$

We deduce $w(x) = \pm\, a(x)\,c(x) = \pm\, P(x)$ or $w(x) = \pm\, a(x)\,c^*(x) = \pm\, P^*(x)$. Contradiction.

**Theorem**

*For any $f \in \mathscr{C}$, $n \geq 3$, denote by*

$$f(x) = A(x)B(x)C(x) = -1 + x + x^n + x^{m_1} + x^{m_2} + \ldots + x^{m_s},$$

*where $s \geq 1$, $m_1 - n \geq n-1$, $m_{j+1} - m_j \geq n-1$ for $1 \leq j < s$, the factorization of $f$ where*

*$A$ is the cyclotomic component,*

*$B$ the reciprocal noncyclotomic component,*

*$C$ the nonreciprocal part.*

*Then $C$ is irreducible.*

(generalizes Selmer's Theorem)
Cor. : $C$ vanishes on the unique zero of $f(x)$ in $(0,1)$ and does not vanish on $|z| = 1$.

Proof : Let us assume that $C$ is reducible, and apply Ljunggren's Lemma. Then there should exist $w(x)$ different of $\pm f(x)$ and $\pm f^*(x)$ such that $w(x)\, w^*(x) = f(x)\, f^*(x)$. For short, we write

$$f(x) = \sum_{j=0}^{r} a_j x^{d_j} \qquad \text{and} \quad w(x) = \sum_{j=0}^{q} b_j x^{k_j}$$

where the coefficients $a_j$ and the exponents $d_j$ are given, and the $b_j$'s and the $k_j$'s are unkown integers, with $|b_j| \geq 1$, $0 \leq j \leq q$,

$$a_0 = -1,\; a_1 = a_2 = \ldots = a_r = 1,$$

$$0 = d_0 < d_1 = 1 < d_2 = n < d_3 = m_1 < \ldots < d_{r-1} = m_{s-1} < d_r = m_s,$$

$$0 = k_0 < k_1 < k_2 < \ldots < k_{q-1} < k_q.$$

The relation $w(x)\,w^*(x) = f(x)\,f^*(x)$ implies the equality : $2k_q = 2d_r$ ; expanding it and considering the terms of degree $k_q = d_r$, we deduce $\|f\|^2 = \|w\|^2 = r+1$ which is equal to $s+3$. Since $f^*(1) = f(1)$ and that $w^*(1) = w(1)$, it also implies $f(1)^2 = w(1)^2$ and $b_0 b_q = -1$. Then we have two equations

$$r-1 = \sum_{j=1}^{q-1} b_j^2, \qquad\qquad (r-1)^2 = (\sum_{j=1}^{q-1} b_j)^2.$$

We will show that they admit no solution except the solution $w(x) = \pm f(x)$ or $= \pm f^*(x)$.

Since all $|b_j|$'s are $\geq 1$, the inequality $q \leq r$ necessarily holds. If $q = r$, then the $b_j$'s should all be equal to $-1$ or $+1$, what corresponds to $\pm f(x)$ or to $\pm f^*(x)$. If $2 \leq q < r$, the maximal value taken by a coefficient $b_j^2$ is equal to the largest square less than or equal to $r - q + 1$, so that $|b_j| \leq \sqrt{r - q + 1}$. Therefore there is no solution for the cases "$q = r - 1$" and "$q = r - 2$". If $q = r - 3$ all $b_j^2$'s are equal to 1 except one equal to 4, and

$$r - 1 = \sum_{j=1}^{r-4} b_j^2, \qquad (r-1)^2 > (\sum_{j=1}^{r-4} b_j)^2.$$

This means that the case "$q = r - 3$" is impossible. The two cases "$q = r - 4$" and "$q = r - 5$" are impossible since, for $m = 5$ and 6, $\sum_{j=1}^{r-m} b_j^2$ cannot be equal to $r - 1$. This is general. For $q \leq r - 3$ at least one of the $|b_j|$'s is equal to 2 ; in this case we would have

$$r - 1 = \pm \sum_{j=1}^{q-1} b_j \leq \sum_{j=1}^{q-1} |b_j| < \sum_{j=1}^{q-1} b_j^2 = r - 1.$$

Contradiction.

**Theorem**

*Suppose $f(x) \in \mathscr{C}$ of the form*

$$-1 + x + x^n + x^{m_1} + \ldots + x^{m_s}, \quad n \geq 3,\ s \geq 1.$$

*Then the number $\omega(f)$, resp. $\omega_1(f)$, of irreducible factors, resp. of irreducible noncyclotomic factors, of $f(x)$ counted without multiplicities in both cases, satisfy*

*(i)*

$$\omega(f) \ll \sqrt{\frac{m_s \operatorname{Log}(s+3)}{\operatorname{Log}\operatorname{Log} m_s}} \qquad (m_s \to \infty),$$

*(ii) for every $\varepsilon \in (0,1)$,*

$$\omega_1(f) = o(m_s^{\varepsilon})\,(\operatorname{Log}(s+3))^{1-\varepsilon}, \qquad (m_s \to \infty).$$

The bounds given by Schinzel's Theorem are quite large.

Result (heuristics) :

75 % of the polynomials $P \in \mathscr{C}$ are irreducible,
i.e. are reduced to their non-reciprocal component.

Remaining cases, found : the other factors are cyclotomic.

## Examples :

$$P(x) := (-1 + x + x^{37}) + x^{81} + x^{140} + x^{184} + x^{232} + x^{285} + x^{350} + x^{389} + x^{450} + x^{514} + x^{550} + x^{590} + x^{649}$$

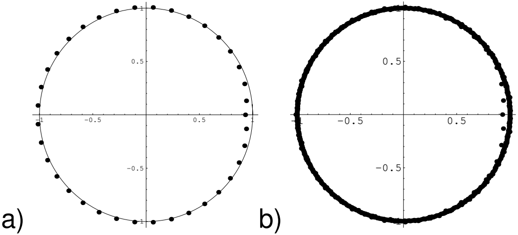


FIGURE: a) The 37 zeroes of $G_{37}(x) = -1 + x + x^{37}$, b) The 649 zeroes of $P(x) = G_{37}(x) + \ldots + x^{649}$. The lenticulus of roots of $P$ is obtained by a very slight deformation of the restriction of the lenticulus of roots of $G_{37}$ to the angular sector $|\arg z| < \pi/18$, off the unit circle. The other roots (nonlenticular) of $P$ can be found in a narrow annular neighbourhood of $|z| = 1$.

The lenticulus of roots is a lenticulus of conjugates of the real zero $\in (0,1)$ of $C$ in

### Theorem

*For any $f \in \mathscr{C}$, $n \geq 3$, denote by*

$$f(x) = A(x)B(x)C(x) = -1 + x + x^n + x^{m_1} + x^{m_2} + \ldots + x^{m_s},$$

*where $s \geq 1$, $m_1 - n \geq n-1$, $m_{j+1} - m_j \geq n-1$ for $1 \leq j < s$, the factorization of $f$ where*

*$A$ is the cyclotomic component,*

*$B$ the reciprocal noncyclotomic component,*

*$C$ the nonreciprocal part.*

*Then $C$ is irreducible.*

Cor. : $C$ vanishes on the unique zero of $f(x)$ in $(0,1)$ and does not vanish on $|z| = 1$.

# Other examples

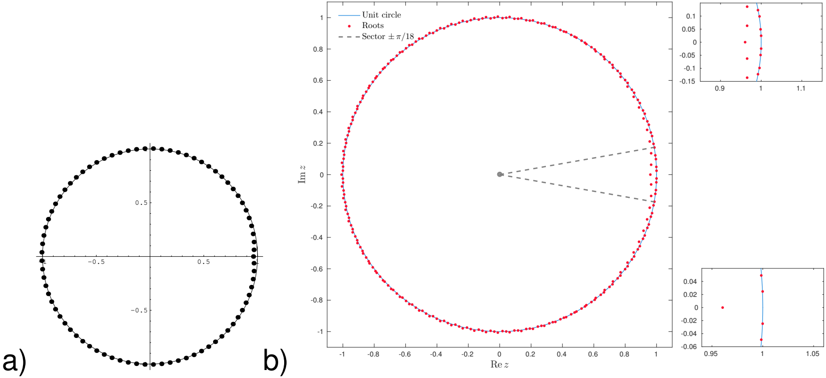


FIGURE: a) Zeroes of $G_{81}$, b) Zeroes of $P(x) = -1 + x + x^{81} + x^{165} + x^{250}$. On the right the distribution of the roots of $P$ is zoomed twice in the angular sector $-\pi/18 < \arg(z) < \pi/18$.

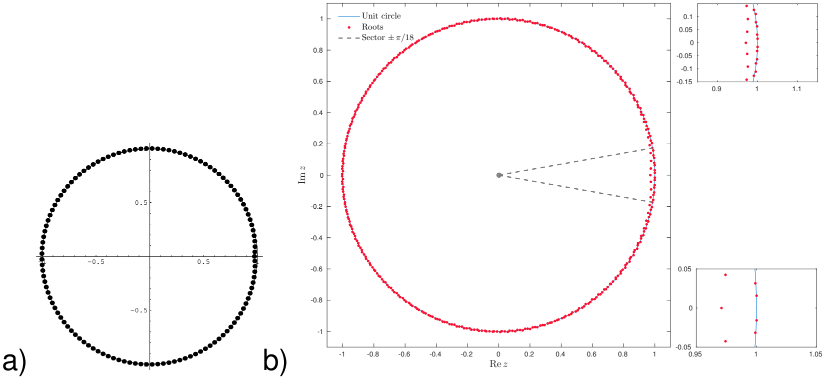


FIGURE: a) Zeroes of $G_{121}$, b) Zeroes of $f(x) = -1 + x + x^{121} + x^{250} + x^{385}$. On the right the distribution of the roots of $f$ is zoomed twice in the angular sector $-\pi/18 < \arg(z) < \pi/18$.

Denote by $\beta > 1$ the real number such that

$$C(\beta^{-1}) = 0,$$

where

$$P(x) = A(x)B(x)C(x) = -1 + x + x^n + x^{m_1} + x^{m_2} + \ldots + x^{m_s},$$

where $s \geq 1$, $m_1 - n \geq n - 1$, $m_{j+1} - m_j \geq n - 1$ for $1 \leq j < s$, the factorization of $P$.

Next Lecture : Introduce the $\beta$-transformation $T_\beta$ and the properties of the Rényi dynamical systems for varying $\beta$s :

$$([0,1], T_\beta)$$