

How random are Legendre symbols?

Youness Lamzouri
University of Lorraine

NuTMiC 2026
University of Silesia, September 21, 2026

The Legendre symbol

- Here and throughout, p denotes an odd prime number.
- The **Legendre symbol** is defined by

$$\chi_p(a) = \left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a non-zero square modulo } p, \\ -1 & \text{if } a \text{ is not a square modulo } p, \\ 0 & \text{if } p \mid a. \end{cases}$$

The Legendre symbol

- Here and throughout, p denotes an odd prime number.
- The **Legendre symbol** is defined by

$$\chi_p(a) = \left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a non-zero square modulo } p, \\ -1 & \text{if } a \text{ is not a square modulo } p, \\ 0 & \text{if } p \mid a. \end{cases}$$

- For example, when $p = 7$, we have

a	1	2	3	4	5	6
$\chi_7(a)$	1	1	-1	1	-1	-1

The Legendre symbol

- Here and throughout, p denotes an odd prime number.
- The **Legendre symbol** is defined by

$$\chi_p(a) = \left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a non-zero square modulo } p, \\ -1 & \text{if } a \text{ is not a square modulo } p, \\ 0 & \text{if } p \mid a. \end{cases}$$

- For example, when $p = 7$, we have

a	1	2	3	4	5	6
$\chi_7(a)$	1	1	-1	1	-1	-1

Question

In what sense does this deterministic sequence behave like random signs?

Basic properties of the Legendre symbol

- The Legendre symbol is **periodic modulo p** :

$$\chi_p(a + p) = \chi_p(a).$$

Basic properties of the Legendre symbol

- The Legendre symbol is **periodic modulo p** :

$$\chi_p(a + p) = \chi_p(a).$$

- It is **completely multiplicative**:

$$\chi_p(ab) = \chi_p(a)\chi_p(b).$$

Basic properties of the Legendre symbol

- The Legendre symbol is **periodic modulo p** :

$$\chi_p(a + p) = \chi_p(a).$$

- It is **completely multiplicative**:

$$\chi_p(ab) = \chi_p(a)\chi_p(b).$$

Quadratic reciprocity (Gauss, 1801)

For distinct odd primes p and q ,

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.$$

We also have $\chi_p(-1) = (-1)^{(p-1)/2}$.

Randomness of the Legendre symbol

- For independent random signs, every pattern of length k occurs with probability 2^{-k} .

Randomness of the Legendre symbol

- For independent random signs, every pattern of length k occurs with probability 2^{-k} .
- Do we see the same pattern frequencies in the Legendre sequence?

Randomness of the Legendre symbol

- For independent random signs, every pattern of length k occurs with probability 2^{-k} .
- Do we see the same pattern frequencies in the Legendre sequence?

Theorem (Davenport, 1933)

Fix k and signs $\varepsilon_0, \dots, \varepsilon_{k-1}$. Then

$$\frac{1}{p} \#\{a \bmod p : \chi_p(a+j) = \varepsilon_j, \text{ for all } 0 \leq j \leq k-1\} = \frac{1}{2^k} + o(1).$$

In particular, each fixed pattern occurs with frequency tending to 2^{-k} .

This is a **statistical** form of pseudorandomness.

Applications in cryptography

- **Damgård (1988)** proposed the shifted Legendre sequence

$$\chi_p(K), \chi_p(K+1), \chi_p(K+2), \dots$$

as a pseudorandom bit generator, where p is public and $K \in \mathbb{F}_p$ is secret.

Applications in cryptography

- **Damgård (1988)** proposed the shifted Legendre sequence

$$\chi_p(K), \chi_p(K+1), \chi_p(K+2), \dots$$

as a pseudorandom bit generator, where p is public and $K \in \mathbb{F}_p$ is secret.

- **Grassi–Rechberger–Rotaru–Scholl–Smart (2016)** revisited the associated **Legendre pseudorandom function**

$$L_{p,K}(n) = \left\lfloor \frac{1 - \chi_p(K+n)}{2} \right\rfloor, \quad n \in \mathbb{F}_p.$$

Applications in cryptography

- **Damgård (1988)** proposed the shifted Legendre sequence

$$\chi_p(K), \chi_p(K+1), \chi_p(K+2), \dots$$

as a pseudorandom bit generator, where p is public and $K \in \mathbb{F}_p$ is secret.

- **Grassi–Rechberger–Rotaru–Scholl–Smart (2016)** revisited the associated **Legendre pseudorandom function**

$$L_{p,K}(n) = \left\lfloor \frac{1 - \chi_p(K+n)}{2} \right\rfloor, \quad n \in \mathbb{F}_p.$$

- Thus one obtains the following **hidden-shift problem**: given oracle access to $\mathcal{O}_K(n) = L_{p,K}(n)$, can one recover the unknown shift K ?

Applications in cryptography

- **Damgård (1988)** proposed the shifted Legendre sequence

$$\chi_p(K), \chi_p(K+1), \chi_p(K+2), \dots$$

as a pseudorandom bit generator, where p is public and $K \in \mathbb{F}_p$ is secret.

- **Grassi–Rechberger–Rotaru–Scholl–Smart (2016)** revisited the associated **Legendre pseudorandom function**

$$L_{p,K}(n) = \left\lfloor \frac{1 - \chi_p(K+n)}{2} \right\rfloor, \quad n \in \mathbb{F}_p.$$

- Thus one obtains the following **hidden-shift problem**: given oracle access to $\mathcal{O}_K(n) = L_{p,K}(n)$, can one recover the unknown shift K ?
- **Khovratovich (2019)** obtained a key-recovery algorithm with complexity $O(\sqrt{p} \log p)$.

Legendre paths

- We define γ_p to be the polygonal path obtained by linearly joining the points $(j, z_p(j))$ and $(j+1, z_p(j+1))$, for $0 \leq j \leq p-1$, where

$$z_p(j) = \frac{1}{\sqrt{p}} \sum_{n=0}^j \left(\frac{n}{p} \right).$$

Legendre paths

- We define γ_p to be the polygonal path obtained by linearly joining the points $(j, z_p(j))$ and $(j+1, z_p(j+1))$, for $0 \leq j \leq p-1$, where

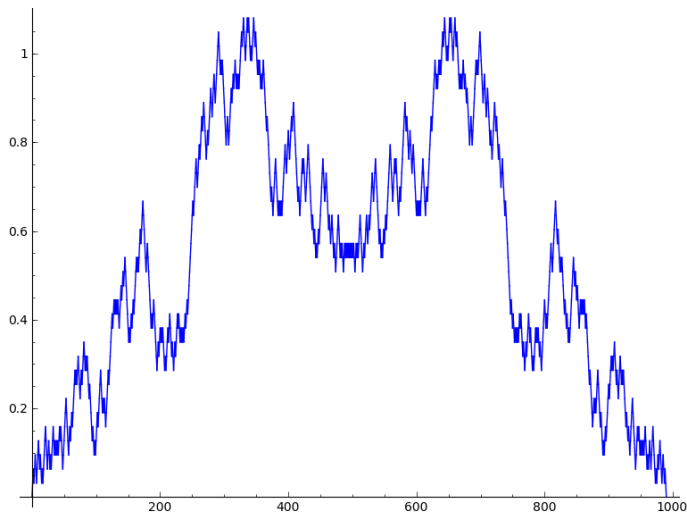
$$z_p(j) = \frac{1}{\sqrt{p}} \sum_{n=0}^j \left(\frac{n}{p} \right).$$

- Note that $z_p(0) = 0$ and

$$z_p(p-1) = \frac{1}{\sqrt{p}} \sum_{n=0}^{p-1} \left(\frac{n}{p} \right) = 0,$$

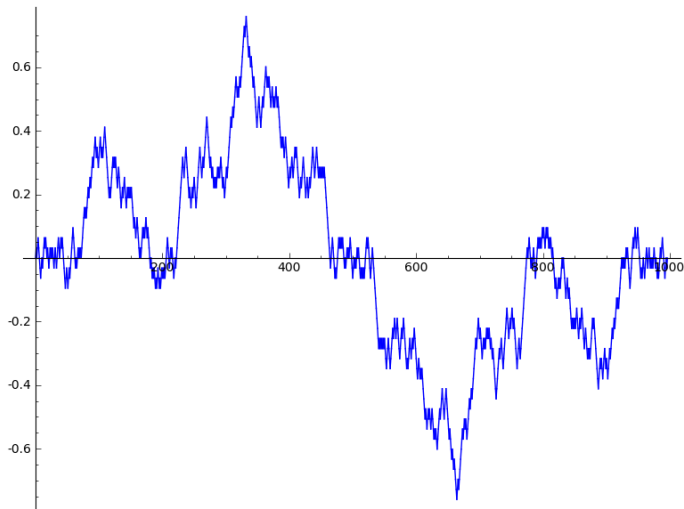
since there are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues among the residue classes $1, 2, 3, \dots, p-1$ modulo p .

The Legendre path for $p = 991 \equiv 3 \pmod{4}$



Horizontal coordinate in the original picture: pt .

The Legendre path for $p = 997 \equiv 1 \pmod{4}$



Horizontal coordinate in the original picture: $pt.$

Questions about Legendre paths

The paths have an arithmetic symmetry:

$$z_p(p-1-j) = -\chi_p(-1)z_p(j).$$

Questions about Legendre paths

The paths have an arithmetic symmetry:

$$z_p(p-1-j) = -\chi_p(-1)z_p(j).$$

- When does the path **first go down**? This is the **least quadratic non-residue problem**.

Questions about Legendre paths

The paths have an arithmetic symmetry:

$$z_p(p-1-j) = -\chi_p(-1)z_p(j).$$

- When does the path **first go down**? This is the **least quadratic non-residue problem**.
- How **high** can it go? How is its maximum distributed as p varies?

Questions about Legendre paths

The paths have an arithmetic symmetry:

$$z_p(p-1-j) = -\chi_p(-1)z_p(j).$$

- When does the path **first go down**? This is the **least quadratic non-residue problem**.
- How **high** can it go? How is its maximum distributed as p varies? Equivalently, this amounts to studying the maximum of character sums.

Questions about Legendre paths

The paths have an arithmetic symmetry:

$$z_p(p-1-j) = -\chi_p(-1)z_p(j).$$

- When does the path **first go down**? This is the **least quadratic non-residue problem**.
- How **high** can it go? How is its maximum distributed as p varies? Equivalently, this amounts to studying the maximum of character sums.
- How are the Legendre paths **distributed** as p varies among the primes $\leq x$ and $x \rightarrow \infty$?

Questions about Legendre paths

The paths have an arithmetic symmetry:

$$z_p(p-1-j) = -\chi_p(-1)z_p(j).$$

- When does the path **first go down**? This is the **least quadratic non-residue problem**.
- How **high** can it go? How is its maximum distributed as p varies? Equivalently, this amounts to studying the maximum of character sums.
- How are the Legendre paths **distributed** as p varies among the primes $\leq x$ and $x \rightarrow \infty$? Do we obtain a *nice* limiting distribution?

Questions about Legendre paths

The paths have an arithmetic symmetry:

$$z_p(p-1-j) = -\chi_p(-1)z_p(j).$$

- When does the path **first go down**? This is the **least quadratic non-residue problem**.
- How **high** can it go? How is its maximum distributed as p varies? Equivalently, this amounts to studying the maximum of character sums.
- How are the Legendre paths **distributed** as p varies among the primes $\leq x$ and $x \rightarrow \infty$? Do we obtain a *nice* limiting distribution? Is it a Brownian motion for example?

When does the path first go down?

- Let n_p be the **least quadratic non-residue** modulo p :

$$n_p = \min\{n \geq 1 : \chi_p(n) = -1\}.$$

- How long can the Legendre sequence begin with only $+1$'s?

When does the path first go down?

- Let n_p be the **least quadratic non-residue** modulo p :

$$n_p = \min\{n \geq 1 : \chi_p(n) = -1\}.$$

- How long can the Legendre sequence begin with only $+1$'s?

Theorem (Burgess, 1957)

For every $\varepsilon > 0$, we have

$$n_p \leq C_\varepsilon p^{1/(4\sqrt{e})+\varepsilon}, \quad \frac{1}{4\sqrt{e}} = 0.1516\dots$$

When does the path first go down?

- Let n_p be the **least quadratic non-residue** modulo p :

$$n_p = \min\{n \geq 1 : \chi_p(n) = -1\}.$$

- How long can the Legendre sequence begin with only $+1$'s?

Theorem (Burgess, 1957)

For every $\varepsilon > 0$, we have

$$n_p \leq C_\varepsilon p^{1/(4\sqrt{e})+\varepsilon}, \quad \frac{1}{4\sqrt{e}} = 0.1516\dots$$

Vinogradov's conjecture

For every $\varepsilon > 0$, there is a constant C_ε such that

$$n_p \leq C_\varepsilon p^\varepsilon.$$

Theorem (Ankeny, 1952)

Assuming the **Generalized Riemann Hypothesis GRH**,

$$n_p = O((\log p)^2).$$

Theorem (Ankeny, 1952)

Assuming the **Generalized Riemann Hypothesis GRH**,

$$n_p = O((\log p)^2).$$

Theorem (L., Li and Soundararajan, 2015)

Assuming GRH, for every prime $p \geq 5$,

$$n_p < (\log p)^2.$$

Theorem (Ankeny, 1952)

Assuming the **Generalized Riemann Hypothesis GRH**,

$$n_p = O((\log p)^2).$$

Theorem (L., Li and Soundararajan, 2015)

Assuming GRH, for every prime $p \geq 5$,

$$n_p < (\log p)^2.$$

- Assuming the GRH, Ankeny's bound for n_p implies that the **Miller-Rabin Primality test (1976-1980)** (also called the strong pseudo-prime test) runs in time $O((\log p)^4 \log \log p)$.

The maximum of a Legendre path

Let

$$M(p) = \frac{1}{\sqrt{p}} \max_{0 \leq x \leq p} \left| \sum_{n \leq x} \chi_p(n) \right|.$$

Theorem (Pólya–Vinogradov, 1918)

$$M(p) \leq C \log p.$$

The maximum of a Legendre path

Let

$$M(p) = \frac{1}{\sqrt{p}} \max_{0 \leq x \leq p} \left| \sum_{n \leq x} \chi_p(n) \right|.$$

Theorem (Pólya–Vinogradov, 1918)

$$M(p) \leq C \log p.$$

Theorem (Montgomery and Vaughan, 1977), assuming GRH

$$M(p) \leq C_1 \log \log p.$$

The maximum of a Legendre path

Let

$$M(p) = \frac{1}{\sqrt{p}} \max_{0 \leq x \leq p} \left| \sum_{n \leq x} \chi_p(n) \right|.$$

Theorem (Pólya–Vinogradov, 1918)

$$M(p) \leq C \log p.$$

Theorem (Montgomery and Vaughan, 1977), assuming GRH

$$M(p) \leq C_1 \log \log p.$$

Paley (1932), with Linnik (1944) for prime moduli

There are infinitely many primes p for which

$$M(p) \geq c_2 \log \log p.$$

Randomness over moving intervals

Choose x uniformly modulo p , and consider

$$Y_{p,H}(x) = \frac{1}{\sqrt{H}} \sum_{x < n \leq x+H} \chi_p(n).$$

Theorem (Davenport and Erdős, 1952)

If $H \rightarrow \infty$ and $\log H = o(\log p)$, then $Y_{p,H}$ converges to the standard Gaussian distribution (with mean 0 and variance 1), as $p \rightarrow \infty$.

Randomness over moving intervals

Choose x uniformly modulo p , and consider

$$Y_{p,H}(x) = \frac{1}{\sqrt{H}} \sum_{x < n \leq x+H} \chi_p(n).$$

Theorem (Davenport and Erdős, 1952)

If $H \rightarrow \infty$ and $\log H = o(\log p)$, then $Y_{p,H}$ converges to the standard Gaussian distribution (with mean 0 and variance 1), as $p \rightarrow \infty$.

Theorem (Harper, 2022)

- For every fixed $A > 0$, put $H = \lfloor p/(\log p)^A \rfloor$. Then $Y_{p,H}$ does not converge to the standard Gaussian distribution as $p \rightarrow \infty$ through the primes.

Randomness over moving intervals

Choose x uniformly modulo p , and consider

$$Y_{p,H}(x) = \frac{1}{\sqrt{H}} \sum_{x < n \leq x+H} \chi_p(n).$$

Theorem (Davenport and Erdős, 1952)

If $H \rightarrow \infty$ and $\log H = o(\log p)$, then $Y_{p,H}$ converges to the standard Gaussian distribution (with mean 0 and variance 1), as $p \rightarrow \infty$.

Theorem (Harper, 2022)

- For every fixed $A > 0$, put $H = \lfloor p/(\log p)^A \rfloor$. Then $Y_{p,H}$ does not converge to the standard Gaussian distribution as $p \rightarrow \infty$ through the primes.
- There is a sequence of primes along which the Gaussian model fails.

A random model for Legendre paths

For simplicity, consider primes $p \equiv 3 \pmod{4}$.

- Let $\{\mathbb{X}(\ell)\}_{\ell \text{ prime}}$ be independent random signs, and extend $\mathbb{X}$ by complete multiplicativity:

$$\mathbb{X}(n) = \prod_{\ell^a \parallel n} \mathbb{X}(\ell)^a.$$

A random model for Legendre paths

For simplicity, consider primes $p \equiv 3 \pmod{4}$.

- Let $\{\mathbb{X}(\ell)\}_{\ell \text{ prime}}$ be independent random signs, and extend $\mathbb{X}$ by complete multiplicativity:

$$\mathbb{X}(n) = \prod_{\ell^a \parallel n} \mathbb{X}(\ell)^a.$$

- We define the following random Fourier series

$$F_{\mathbb{X}}(t) = \frac{1}{\pi} \sum_{n \geq 1} \frac{\mathbb{X}(n)}{n} (1 - \cos(2\pi nt)).$$

A random model for Legendre paths

For simplicity, consider primes $p \equiv 3 \pmod{4}$.

- Let $\{\mathbb{X}(\ell)\}_{\ell \text{ prime}}$ be independent random signs, and extend $\mathbb{X}$ by complete multiplicativity:

$$\mathbb{X}(n) = \prod_{\ell^a \parallel n} \mathbb{X}(\ell)^a.$$

- We define the following random Fourier series

$$F_{\mathbb{X}}(t) = \frac{1}{\pi} \sum_{n \geq 1} \frac{\mathbb{X}(n)}{n} (1 - \cos(2\pi nt)).$$

Theorem (Hussain and L., 2024)

Choose p uniformly among primes in $[Q, 2Q]$ with $p \equiv 3 \pmod{4}$. As $Q \rightarrow \infty$, the Legendre paths γ_p converge in law in $C([0, 1])$ to $F_{\mathbb{X}}$.

The random series describes the statistics of the whole curve.

Littlewood polynomials

- A **Littlewood polynomial** is a polynomial whose coefficients are in $\{-1, 1\}$:

$$P(z) = \sum_{n=0}^{N-1} \varepsilon_n z^n, \quad \varepsilon_n \in \{-1, 1\}.$$

Littlewood's conjecture (1966), proved in 2020

Balister, Bollobás, Morris, Sahasrabudhe and Tiba: there exist absolute constants $c, C > 0$ such that, for every $N \geq 3$, there exists a Littlewood polynomial P_N with degree N such that

$$c\sqrt{N} \leq |P(z)| \leq C\sqrt{N} \quad \text{for all } |z| = 1.$$

Littlewood polynomials

- A **Littlewood polynomial** is a polynomial whose coefficients are in $\{-1, 1\}$:

$$P(z) = \sum_{n=0}^{N-1} \varepsilon_n z^n, \quad \varepsilon_n \in \{-1, 1\}.$$

Littlewood's conjecture (1966), proved in 2020

Balister, Bollobás, Morris, Sahasrabudhe and Tiba: there exist absolute constants $c, C > 0$ such that, for every $N \geq 3$, there exists a Littlewood polynomial P_N with degree N such that

$$c\sqrt{N} \leq |P(z)| \leq C\sqrt{N} \quad \text{for all } |z| = 1.$$

Erdős's Ultra-flatness conjecture (1957)

There is an absolute $\delta > 0$ such that every Littlewood polynomial with degree $N \geq 2$ satisfies

$$\max_{|z|=1} |P(z)| \geq (1 + \delta)\sqrt{N}.$$

The L^q norms of random polynomials

Here and throughout, we put $e(t) = e^{2\pi it}$.

The L^q norms of random polynomials

Here and throughout, we put $e(t) = e^{2\pi it}$. For $q > 0$, define

$$\|P\|_q = \left(\int_0^1 |P(e(t))|^q dt \right)^{1/q}.$$

For a degree $N - 1$ Littlewood polynomial P_N , Parseval gives $\|P\|_2 = \sqrt{N}$.

The L^q norms of random polynomials

Here and throughout, we put $e(t) = e^{2\pi it}$. For $q > 0$, define

$$\|P\|_q = \left(\int_0^1 |P(e(t))|^q dt \right)^{1/q}.$$

For a degree $N-1$ Littlewood polynomial P_N , Parseval gives $\|P\|_2 = \sqrt{N}$.

Borwein and Lockhart (2001)

For a random Littlewood polynomial $P(z) = \sum_{n=0}^{N-1} \varepsilon_n z^n$, where $\varepsilon_0, \dots, \varepsilon_{N-1}$ are independent random variables taking the values ± 1 with probability $1/2$, we have

$$\mathbb{E} \frac{\|P\|_q}{\sqrt{N}} \longrightarrow (\mathbb{E}|Z|^q)^{1/q} = \Gamma(1 + q/2)^{1/q},$$

where Z is a standard complex Gaussian with $\mathbb{E}|Z|^2 = 1$.

Fekete polynomials

- The **Fekete polynomial** attached to p is defined by

$$F_p(z) = \sum_{n=1}^{p-1} \chi_p(n) z^n.$$

- The polynomial $F_p(z)/z$ is a Littlewood polynomial.

Gauss sum evaluation (1811)

For $1 \leq k \leq p-1$,

$$F_p(e(k/p)) = \chi_p(k) \tau_p, \quad \tau_p = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod{4}, \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Fekete polynomials

- The **Fekete polynomial** attached to p is defined by

$$F_p(z) = \sum_{n=1}^{p-1} \chi_p(n) z^n.$$

- The polynomial $F_p(z)/z$ is a Littlewood polynomial.

Gauss sum evaluation (1811)

For $1 \leq k \leq p-1$,

$$F_p(e(k/p)) = \chi_p(k) \tau_p, \quad \tau_p = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod{4}, \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

- Thus $|F_p(e(k/p))| = \sqrt{p}$ at every non-trivial p -th root of unity.

Fekete polynomials

- The **Fekete polynomial** attached to p is defined by

$$F_p(z) = \sum_{n=1}^{p-1} \chi_p(n) z^n.$$

- The polynomial $F_p(z)/z$ is a Littlewood polynomial.

Gauss sum evaluation (1811)

For $1 \leq k \leq p-1$,

$$F_p(e(k/p)) = \chi_p(k) \tau_p, \quad \tau_p = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod{4}, \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

- Thus $|F_p(e(k/p))| = \sqrt{p}$ at every non-trivial p -th root of unity.
- The discrete Fourier spectrum is perfectly flat. What happens **between** the roots of unity?

The limiting process for Fekete polynomials

For a uniformly chosen $k \bmod p$, we define

$$G_p(k, t) = \frac{F_p(e((k+t)/p))}{\tau_p}, \quad 0 \leq t \leq 1.$$

The limiting process for Fekete polynomials

For a uniformly chosen $k \bmod p$, we define

$$G_p(k, t) = \frac{F_p(e((k+t)/p))}{\tau_p}, \quad 0 \leq t \leq 1.$$

Theorem (Klurman, L. and Munsch, 2023+)

The processes $G_p(k, \cdot)$ converge in law in $C([0, 1])$ to the process

$$G_{\mathbb{X}}(t) = \sum_{m \in \mathbb{Z}} \frac{e(t) - 1}{2\pi i(t - m)} \mathbb{X}(m),$$

where all the $\mathbb{X}(m)$ are independent random variables taking the values ± 1 with probability $1/2$.

The limiting process for Fekete polynomials

For a uniformly chosen $k \bmod p$, we define

$$G_p(k, t) = \frac{F_p(e((k+t)/p))}{\tau_p}, \quad 0 \leq t \leq 1.$$

Theorem (Klurman, L. and Munsch, 2023+)

The processes $G_p(k, \cdot)$ converge in law in $C([0, 1])$ to the process

$$G_{\mathbb{X}}(t) = \sum_{m \in \mathbb{Z}} \frac{e(t) - 1}{2\pi i(t - m)} \mathbb{X}(m),$$

where all the $\mathbb{X}(m)$ are independent random variables taking the values ± 1 with probability $1/2$.

Since $G_{\mathbb{X}}(0) = \mathbb{X}(0) \in \{-1, 1\}$, $G_{\mathbb{X}}$ is **not a Gaussian process**.

The limiting L^q norms of Fekete polynomials

Theorem (Klurman, L. and Munsch, 2023+)

For every fixed $q > 0$,

$$\frac{\|F_p\|_q}{\sqrt{p}} \longrightarrow k_q := \left(\int_0^1 \mathbb{E} |G_{\mathbb{X}}(t)|^q dt \right)^{1/q}.$$

The limiting L^q norms of Fekete polynomials

Theorem (Klurman, L. and Munsch, 2023+)

For every fixed $q > 0$,

$$\frac{\|F_p\|_q}{\sqrt{p}} \longrightarrow k_q := \left(\int_0^1 \mathbb{E} |G_{\mathbb{X}}(t)|^q dt \right)^{1/q}.$$

These are the moments of a **non-Gaussian** model.

The Mahler measure

The Mahler measure is the geometric mean of $|P|$:

$$M(P) = \exp \left(\int_0^1 \log |P(e(t))| dt \right)$$

The Mahler measure

The Mahler measure is the geometric mean of $|P|$:

$$M(P) = \exp \left(\int_0^1 \log |P(e(t))| dt \right) = \lim_{q \rightarrow 0^+} \|P\|_q.$$

The Mahler measure

The Mahler measure is the geometric mean of $|P|$:

$$M(P) = \exp \left(\int_0^1 \log |P(e(t))| dt \right) = \lim_{q \rightarrow 0^+} \|P\|_q.$$

If $P(z) = a \prod_{j=1}^d (z - \alpha_j)$, Jensen's formula gives

$$M(P) = |a| \prod_{j=1}^d \max\{1, |\alpha_j|\}.$$

The Mahler measure

The Mahler measure is the geometric mean of $|P|$:

$$M(P) = \exp \left(\int_0^1 \log |P(e(t))| dt \right) = \lim_{q \rightarrow 0^+} \|P\|_q.$$

If $P(z) = a \prod_{j=1}^d (z - \alpha_j)$, Jensen's formula gives

$$M(P) = |a| \prod_{j=1}^d \max\{1, |\alpha_j|\}.$$

Mahler's problem (1963)

Is there a $\delta > 0$ such that $M(P) \leq (1 - \delta)\sqrt{N}$ for every Littlewood polynomial with degree $N \geq 2$?

The Mahler measure of Fekete polynomials

Theorem (Klurman, L. and Munsch, 2023)

$$\frac{M(F_p)}{\sqrt{p}} \longrightarrow 0.74083\dots$$

This solves the long-standing problem of determining the limiting Mahler measure of Fekete polynomials.

The Mahler measure of Fekete polynomials

Theorem (Klurman, L. and Munsch, 2023)

$$\frac{M(F_p)}{\sqrt{p}} \longrightarrow 0.74083\dots$$

This solves the long-standing problem of determining the limiting Mahler measure of Fekete polynomials.

Theorem (Choi and Erdélyi, 2014)

For a random Littlewood polynomial of degree N the average satisfies

$$\mathbb{E} \frac{M(P)}{\sqrt{N}} \longrightarrow \exp(\mathbb{E} \log |Z|) = e^{-\gamma/2} = 0.749306\dots,$$

where $\gamma = 0.577215\dots$ is the Euler–Mascheroni constant.

The Mahler measure of Fekete polynomials

Theorem (Klurman, L. and Munsch, 2023)

$$\frac{M(F_p)}{\sqrt{p}} \longrightarrow 0.74083\dots$$

This solves the long-standing problem of determining the limiting Mahler measure of Fekete polynomials.

Theorem (Choi and Erdélyi, 2014)

For a random Littlewood polynomial of degree N the average satisfies

$$\mathbb{E} \frac{M(P)}{\sqrt{N}} \longrightarrow \exp(\mathbb{E} \log |Z|) = e^{-\gamma/2} = 0.749306\dots,$$

where $\gamma = 0.577215\dots$ is the Euler–Mascheroni constant.

The constants are close, but **different**.

Turyn polynomials

- **Turyn polynomials** are obtained by cyclically shifting the coefficients of Fekete polynomials:

$$F_{p,r}(z) = \sum_{n=0}^{p-1} \chi_p(n+r)z^n.$$

Turyn polynomials

- **Turyn polynomials** are obtained by cyclically shifting the coefficients of Fekete polynomials:

$$F_{p,r}(z) = \sum_{n=0}^{p-1} \chi_p(n+r)z^n.$$

Theorem (Mossinghoff, 2024+)

For the shift $r = \lfloor p/4 \rfloor$,

$$\frac{M(F_{p,\lfloor p/4 \rfloor})}{\sqrt{p}} \longrightarrow 0.951 \dots$$

Thus these global quantities depend not only on the values of the Legendre symbols, but also on their **cyclic arrangement**.

Thank you for your attention!