On the discriminant of random polynomials

@VaNTAGeSeminar

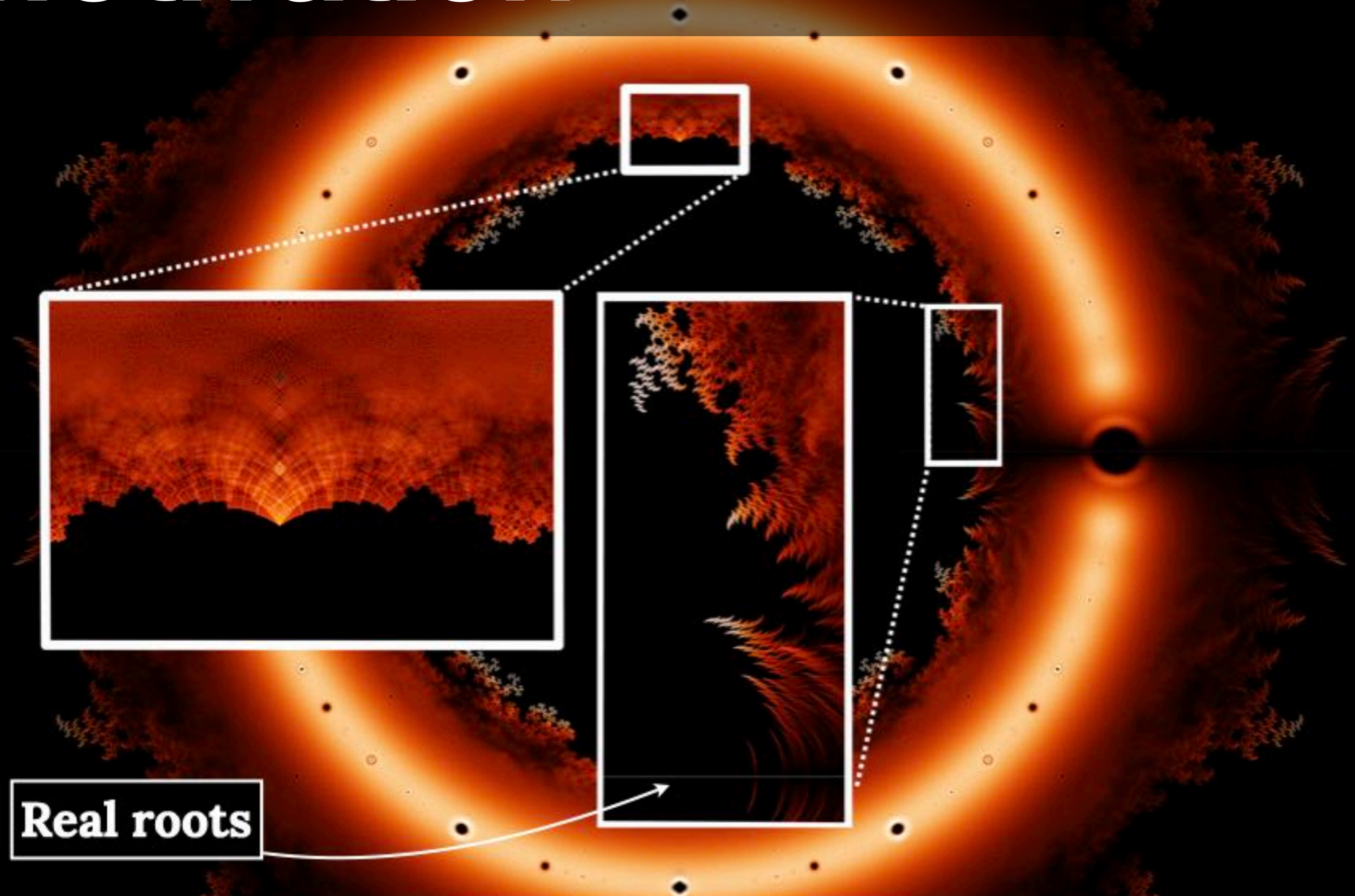
Lior Bary-Soroker, October 17

$$\lim_{n\to\infty} \mathrm{Prob}\left(\mathrm{disc}\left(\sum_{i=0}^{n} \pm X^i\right) = \square\right) = 0?$$

The two open problems of this talk

- For simplicity, I restrict generality to two central special cases
- Let $a_0, a_1, \ldots$ be independent random variables taking values in *uniformly* in $[-L, L] \cap \mathbb{Z} = \{-L, -L+1, \ldots, L\}$
- Our random polynomial is $f = f_{n,L} = X^n + \sum_{i=0}^{n} a_i X^i$
- Put $P_{n,L} = \mathrm{Prob}(\mathrm{disc} f = \square \neq 0)$
- Question 1: How fast $P_{n,L}$ goes to zero as $L \to \infty$?
- Question 2: Does $P_{n,L} \to 0$ as $n \to \infty$? (e.g., $L = 1$)

Motivation



Roots of polynomials with ± 1 coefficients of degree ≤ 24 | **Sam Derbyshire**

The van-der Waerden conjecture

The large box model

$$f = f_{n,L} = X^n + \sum_{i=0}^{n} a_i X^i$$

$$P_{n,L} = \mathrm{Prob}(\mathrm{disc} f = \square \neq 0)$$

- Hilbert, van-der Waerden: $\lim_{L\to\infty} \mathrm{Prob}(G_f = S_n) = 1$
- Van-der Waerden conjecture (1930s): $\mathrm{Prob}(G_f \neq S_n) = \mathrm{Prob}(G_f = S_{n-1}) = O_n(L^{-1}), \quad L \to \infty$
- Knobloch, Gallagher, Zywina, Dietmann, Chow-Dietmann, Anderson-Gafni-Oliver-Lowry—Duda-Shakan-Zhang
- Bhargava's theorem (2021): $\mathrm{Prob}(G_f \neq S_n) = \mathrm{Prob}(G_f = A_n$ or $S_{n-1}) + O_n(L^{-2}) = O_n(L^{-1})$
- **The main breakthrough of Bhargava**: $P_{n,L} = O_n(L^{-1})$

How small is $P_{n,L}$, large box model

naive heuristic

$$f = f_{n,L} = X^n + \sum_{i=0}^{n} a_i X^i$$

$$P_{n,L} = \mathrm{Prob}(\mathrm{disc} f = \square \neq 0)$$

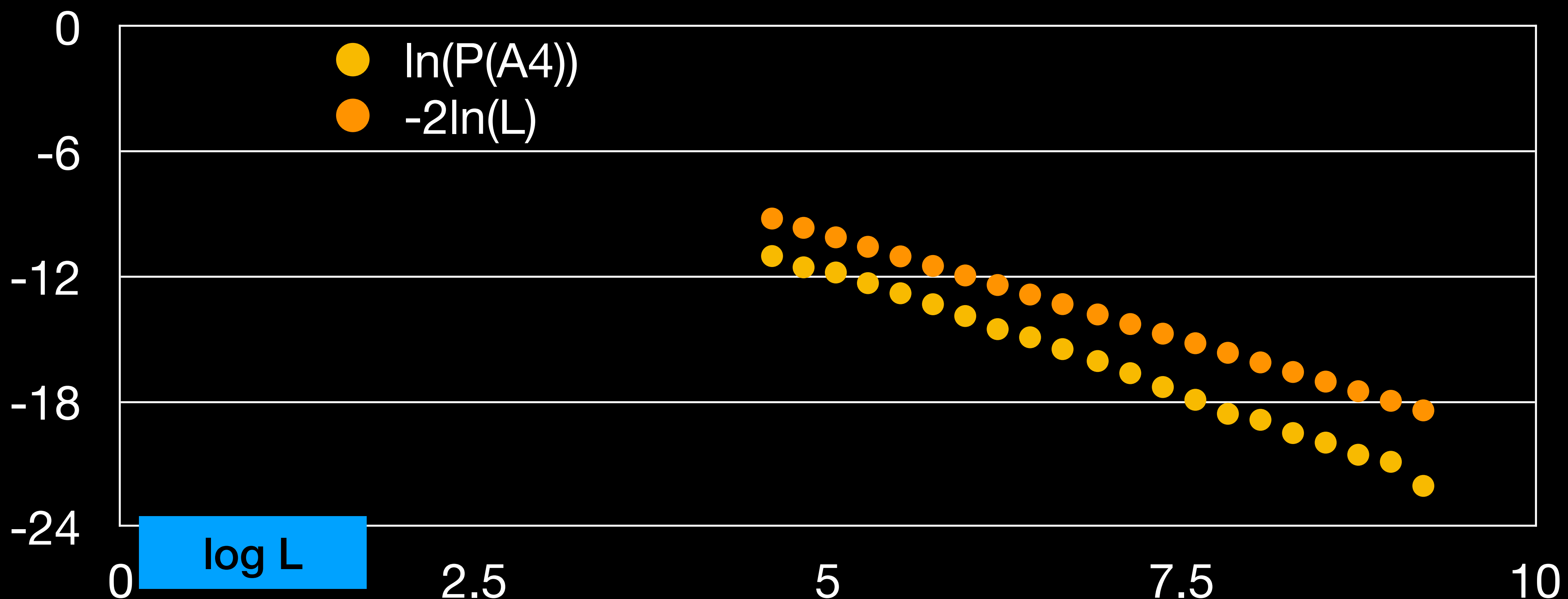
- $\mathrm{disc} f$ is a polynomial is a_i of degree $2n-1$
- Hence $\mathrm{disc} f \approx L^{2n-2}$
- $\mathrm{disc} f$ behaves like a random number
- Probability that a random n is a square is $n^{-1/2}$
- Hence $P_{n,L} \approx L^{1-n}$
- **Wrong heuristic — too small**
- Explanation: $\mathrm{disc} f$ has many symmetries so it is not like random numbers

How small is $P_{n,L}$, large box model
Lower bounds

- $n = 0 \pmod 4, f + f' = g^2 \Rightarrow \mathrm{disc} f = \square$
- LBS-Ben—Porath-Matei: $P_{n,L} \geq \mathrm{Prob}(G_f = A_n) \gg L^{-n/4+\epsilon}$
- LBS-Ben—Porath-Matei: If n is even, then $P_{n,L} \gg L^{-n/2-1/2+\epsilon}$
- In the latter, the Galois group is **never** A_n, it preserves a partition to pairs; i.e., a subgroup of $(C_2 \wr S_{n/2}) \cap A_n$
- We identify a power law: so we will study $-\dfrac{\log P_{n,L}}{\log L}$
- Naive Conjecture: $P_{n,L} \asymp \mathrm{Prob}(G_f = A_n)$

Question 1: How fast $P_{n,L}$ goes to zero as $L \to \infty$?

Conjecture: $$\lim_{L\to\infty} \frac{\log \mathrm{Prob}(G_f = A_n)}{\log L} = -\frac{n}{2}$$



Numerics by Noam Pirani and Ohad Avneri,
last data point: $L = 10^3$, $\approx 10^{11}$ random polynomials, 30 instances of A_4

Odlyzko-Poonen conjecture

Restricted coefficients model

$$f = f_{n,L} = X^n + \sum_{i=0}^{n} a_i X^i$$
$$P_{n,L} = \text{Prob}(\text{disc} f = \square \neq 0)$$

- Odlyzko-Poonen Conjecture, 1993: $\lim_{n\to\infty} \text{Prob}(f \text{ is irreducible} \,|\, f(0) \neq 0) = 1$
- Easy: $\text{Prob}(f \text{ is irreducible} \,|\, f(0) \neq 0) \gg \frac{1}{n}$
- Konyagin,1999: $\text{Prob}(f \text{ is irreducible} \,|\, f(0) \neq 0) \gg \frac{1}{\log n}$
- LBS-Kozma, LBS-Kozma-Koukoulopoulos: $\lim_{n\to\infty} \text{Prob}(f \text{ is irreducible} \,|\, f(0) \neq 0) = 1$ if $L \geq 17$
- Breuillard-Varju: $\lim_{n\to\infty} \text{Prob}(f \text{ is irreducible} \,|\, f(0) \neq 0) = 1$ under GRH
- LBS-Kozma: $\lim_{n\to\infty} \text{Prob}(f \text{ is irreducible} \,|\, f(0) \neq 0) = 1$ implies $\lim_{n\to\infty} \text{Prob}(G_f = A_n \text{ or } S_n) = 1$

Question 2: Does $P_{n,L} \to 0$ as $n \to \infty$?

Positive answer would imply

$$\lim_{n\to\infty} \mathrm{Prob}(G_f = S_n) = 1$$

What is known ?

Finite Fields

Uniform polynomials

- Stickelberger, Swan: $\mu_q(f_q) = (-1)^{\deg f_q} \left(\frac{\mathrm{disc} f_q}{q} \right)$
- Here $\mathbb{F}_q$ is a finite field, $f_q \in \mathbb{F}_q[X]$ a uniform monic polynomial of degree n
- $\left(\frac{a}{q}\right) = \begin{cases} 1 & a = \square \\ -1 & a \neq \square \\ 0 & a = 0 \end{cases}$,
- $\mu_q(f_q) = \begin{cases} (-1)^r & f_q = \prod_{j=1}^r P_j, P_j \text{distinct} \\ 0 & \exists P^2 \mid f \end{cases}$ is the Möbius function
- μ_q^2 is the indicator function for squarefree
- $\mathrm{Prob}(\mu_q = 0,1,-1) = (\frac{1}{q}, \frac{q-1}{2q}, \frac{q-1}{2q})$ for $n > 1$
- Conclusion: $\mathrm{Prob}(\mathrm{disc} f_q = \square \neq 0) = \frac{1}{2} + O(q^{-1})$

Applications

- Corollaries for the large box model:
- Easy: $P_{n,L} \to 0,\ L \to \infty$
- Large sieve inequality: $P_{n,L} \ll \dfrac{n^3}{\sqrt{L}}$
- Bhargava manages to control events mod p^2 and gets $P_{n,L} \le \dfrac{C_n}{L}$
- C_n grows fast with n
- This approach seems to be not applicable in the restricted coefficients model

Finite Fields

Non-uniform polynomials

- Let $a_{iq} \in \mathbb{F}_q$ be independent random variables (e.g., taking the values $-1,0,1$ uniformly) and let $f_q = X^n + \sum_{i=0}^{n-1} a_{iq} X^i$
- How does $\mu_q(f_q)$ distribute? How does $\mu_q^2(f_q)$ distributes?
- Analog questions for the integers: How the Möbius function μ and the indicator function of squarefrees μ^2 distribute on sparse sets of integers (very related: Maynard's theorem on primes with missing digits)
- Work in progress (LBS-Goldgraber): $\mathrm{Prob}(\mathrm{disc} f_p = \square) \approx 1/2$ under mild conditions on the distribution
- Application: The "not-so-large model"

The not-so-large model

$$f = f_{n,L} = X^n + \sum_{i=0}^{n} a_i X^i$$
$$P_{n,L} = \mathrm{Prob}(\mathrm{disc} f = \square \neq 0)$$

- Take $L = L(n)$
- Theorem (LBS-Goldgraber, in progress): If $\lim_{n\to\infty} L(n) = \infty$, $\lim_{n\to\infty} \mathrm{Prob}(G_f = S_n) = 1$
- Idea of the proof:
- If $L \gg n^7$, methods of the large box model gives $\lim_{n\to\infty} \mathrm{Prob}(G_f = S_n) = 1$
- If $L \leq n^7$, then the methods from the restricted coefficients model may be applied, and we get that $\lim_{n\to\infty} \mathrm{Prob}(G_f = A_n \text{ or } S_n) = 1$
- Lemma: $P_{n,L(n)} = o(1)$
- Proof: We use Fourier analysis/exponential sums to compare the distributions of $\mu_p(f \mod p)$ and $\mu_p^2(f \mod p)$ with the respective random variables for uniform polynomials. For μ_p we use tools developed by Sam Porritt and for μ_p^2 we develop new tools

Some words on Fourier analysis

Why it is applicable here?

- $f_p(X) = X^n + \sum_{i=0}^{n-1} a_{ip} X^i$ is a sum of independent variables
- The distribution is then a convolution of measures
- The Fourier coefficients are then a product of Fourier coefficients
- $\hat{f}_p(\chi) = \prod \hat{a}_{ip}(\chi_i)$
- The trivial character is responsible to the contribution of the uniform measure
- The goal is to show that the other coefficients are small
- As $|\hat{a}_{ip}| \leq 1$ it suffices to show that there are “enough” coefficients that are smaller than 1 to be “close” to the uniform distribution
- E.g., in LBS-Koukoulopoulos-Kozma we show that for any non-trivial distribution of the coefficients, there is a constant $\theta > 0$ such that, on average, f_p equidistributes in arithmetic progressions of modulus of degree $\leq \theta n$

Concluding remarks

- In the century of studying probabilistic Galois theory, we have learned that estimating the probability to have a square discriminant is one of the main challenges

- The tools for studying these probabilities are diverse (e.g., algebraic number theory, analytic number theory, finite group theory, combinatorics, random matrix theory,…)

- In recent years, the tool box expanded significantly, by different research groups

- The recent breakthroughs in the subject bring

hope

for further progress on the major open problems

$$\lim_{n\to\infty} \mathrm{Prob}\left(\mathrm{disc}\left(\sum_{i=0}^{n} \pm X^i\right) = \square\right) = 0?$$