Splitting properties of families of S_n-polynomials and application to class group torsion

Let me start with a brief overview of the work I'm going to present.

The goal is to deal with a question in **arithmetic statistics**: the distribution of the "small" splitting primes (in a suitable sense) in families of nb fields.

Notations

$n \geq 3$, $N > 0$ be integers;

$$\mathcal{P}_{n,N} \ni f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X],$$

$a_0, \ldots, a_{n-1}$ are indep., identically uniformely distributed taking values in $\{-N, \ldots, N\}$.

$$ht(f) \leq N. \quad (= \max\{|a_i| \mid i = 0, \ldots, n-1\})$$

We let $N \longrightarrow +\infty$. G_f (= $G_{K_f/\mathbb{Q}}$) are all these f

$$\mathcal{P}^0_{n,N} := \{f \in \mathcal{P}_{n,N} \mid G_{K_f/\mathbb{Q}} \cong S_n\}$$ S_n-polynomials:

K_f = splitting field of f over $\mathbb{Q}$

$G_f \mid n!$

$\mathbb{Q}$

It is well-known that almost all poly are S_n-poly. Recently (Nov. 2021) the **van der Waerden's conjecture** has been proved by Bhargava:

$$|\mathcal{P}_{n,N} \setminus \mathcal{P}^0_{n,N}| \ll N^{n-1} \quad \text{for } n \geq 3.$$

The first step is an effective version on average of the Chebotarev Density Theorem:

$L \supseteq \mathcal{O}_L$ normal extension
$G = \mathrm{Gal}(L|K)$ $\mathcal{C} \subseteq G$ conjugacy class
$K \supseteq \mathcal{O}_K$ $\mathrm{Frob}_{\mathfrak{p},L|K}$ = conj. class in G of the Frobenius automorphism corresponding to $\mathfrak{p}$
$\mathfrak{p}$

$$\pi_{\mathcal{C},L|K}(x) := \sum_{\substack{\mathfrak{p} \subset \mathcal{O}_K,\ N_{K|\mathbb{Q}}\mathfrak{p} \le x \\ \mathfrak{p} \text{ unram. in } L \\ \mathrm{Frob}_{\mathfrak{p},L|K} = \mathcal{C}}} 1 \sim \frac{|\mathcal{C}|}{|G|} \mathrm{Li}(x) \sim \frac{|\mathcal{C}|}{|G|} \frac{x}{\log x}$$

In applications it is highly desirable to have an effective form, that is an explicit error term.
Such an effective thm was proved by Lagarias and Odlyzko under GRH.
We work unconditional, by using the average properties of our family of polynomials.

$f \in \mathcal{P}^0_{n,N}$, $\tau = (\tau_1, \dots, \tau_n)$ splitting type of f modulo a prime p if $f \bmod p$ splits into distinct monic irreducible factors with τ_1 linear factors, τ_2 quadratic and so on.
We consider square-free factorizations.

If $p \nmid D_f$, τ corresponds to the cycle structure of the Frob. element $\mathrm{Frob}_{f,p}$ acting on the roots of f.

Let $\mathcal{C}_\tau$ be the conj. class in S_n of elements of cycle type τ.

$$|\mathcal{C}_\tau| = n!\,\delta(\tau) = n! \prod_{i=1}^{m} \frac{1}{i^{\tau_i}\tau_i!}.$$

$$\pi_{f,\tau}(x) := \sum_{\substack{p \le x \\ f \text{ of spl. type} \\ \tau \bmod p}} 1 = \sum_{p \le x} \mathbb{1}_{f,\tau}(p)$$

↓ sum of random variables on $\mathcal{P}^0_{n,N} \subseteq [-N,N]^n$ sublattice.

Prop: For $\tau < N^{1/n+1}$, the mean value

$$\mathbb{E}_N(\pi_{f,\tau}(x)) = \delta(\tau)\pi(x) + C\,\frac{x}{\log x\log\tau} + O_n(1)$$

as $x, N \to +\infty$.

↓ average version of the CDT

Once proved that the normal order of $\pi_{f,\tau}(x)$ is $\delta(\tau)\pi(x)$, we study the distribution of

$$\frac{\pi_{f,\tau}(x) - \delta(\tau)\pi(x)}{(\delta(\tau)-\delta(\tau)^2)^{1/2}\pi(x)^{1/2}}$$

↓ sqrt of the variance

Erdős–Kac thm:
$$\frac{\omega(m) - \log\log m}{\sqrt{\log\log m}}$$

It turns out that this quantity is distributed like a normal distribution with mean 0 and variance 1.

Thm: For $\tau = N^{1/\log\log N}$ and for any $b \in \mathbb{R}$,

$$\mathbb{P}_N\left(\frac{\pi_{f,\tau}(x) - \delta(\tau)\pi(x)}{(\delta(\tau)-\delta(\tau)^2)^{1/2}\pi(x)^{1/2}} \le b\right) \xrightarrow[N\to+\infty]{} \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{b} e^{-t^2/2}\,dt.$$

EXAMPLE: Primes splitting completely ($\mathcal{C}_\ell = 1$)

$n=3$, $N \approx 10^2$ ($x \approx 20$), the ratio is approximately

$$\pi_{f,\ell}(x) - 1.11$$

which lies in the interval $[-0.9, 0.9]$ iff $\pi_{f,\ell}(x)$ is in $[0.21, 2.01] \sim [0,3]$.

The proportion of cubic S_3-poly with integer coefficients in a box $[-100, 100]$ having between 0 and 3 primes below 20 splitting completely is about 60%.

Application: Bound for ℓ-torsion of class groups

$K/\mathbb{Q}$ nb field of degree d, discriminant D_K

Cl_K = ideal class group
finite abelian group that encodes information about the arithmetic of K

$h_K = |Cl_K|$ = class number

We focus on the ℓ-torsion subgroups, $\ell \geq 1$:

$$Cl_K[\ell] := \{[\alpha] \in Cl_K \mid [\alpha]^\ell = 1d\}$$

$$h_K[\ell] := |Cl_K[\ell]|.$$

Landau observed the upper bound

$$h_K[\ell] \ll_{d,\varepsilon} D_K^{1/2+\varepsilon} \quad \forall \varepsilon > 0$$

It is thought to be far from the truth.

CONJ. (ℓ-torsion Conjecture) : $\forall \varepsilon > 0$, $h_K[\ell] \ll_{d,\ell,\varepsilon} D_K^{\varepsilon}$.
or ε- conjecture

Results in the direction of the ℓ-torsion conjecture.

(Soundararajan): For all but a possible 0-density family of exceptional imaginary quadratic fields,

$$h_K[\ell] \ll_{\ell,\varepsilon} D_K^{1/2 - 1/2\ell + \varepsilon} \quad \forall \varepsilon > 0.$$

$\downarrow$

$|\mathcal{F}_{\mathrm{disc} \le X}| \gg X^{\beta}$
$|\mathcal{E}_{\mathrm{disc} \le X}| \ll X^{\alpha}$
$0 \le \alpha < \beta$

(Heath-Brown): For almost all quadratic fields,

$$h_K[\ell] \ll_{\ell,\varepsilon} D_K^{1/2 - 3/(2\ell+2) + \varepsilon} \quad \forall \varepsilon > 0.$$

(Ellenberg-Venkatesh): Under GRH,

$$h_K[\ell] \ll_{d,\ell,\varepsilon} D_K^{1/2 - \frac{1}{2\ell(d-1)} + \varepsilon} \quad \forall \varepsilon > 0.$$

The main point for $\uparrow$ is the existence of many primes splitting completely. The GRH guarantees the existence of many such primes.

COROLL: For any $\ell \ge 1$ integer,

$$h_{K_f}[\ell] \ll_{m,\ell,\varepsilon} D_{K_f}^{\frac{1}{2} - \frac{1}{(2m-2)(m-1)! \log\log d_f} + \varepsilon} \cdot \frac{\log N}{\log\log N}$$

$\forall \varepsilon > 0$, for almost all $f \in \mathcal{B}_{2,N}^{0}$.

d_f = discriminant of f.