2. Random primes

Thm 2.1 (PNT for arithmetic progressions)

For any $a \in (\mathbb{Z}/n\mathbb{Z})^\times$,

$$\mathbb{P}_{p \text{ prime}}(p \equiv a \bmod n) = \frac{1}{\varphi(n)} = \frac{1}{\#(\mathbb{Z}/n\mathbb{Z})^\times}.$$

~~Thm 2.2 (Chebotarev density thm)~~

Let $L|K$ be a fin. Gal. ext. with Gal group G.

~~For any unram. primes $\mathfrak{P}|\mathfrak{p}$ of $L|K$, Frob we have a~~

For any unram. prime $\mathfrak{p}$ of K,

$$\mathrm{Frob}(\mathfrak{p}) := \{\mathrm{Frob}(\mathfrak{P}|\mathfrak{p}) : \mathfrak{P}|\mathfrak{p} \text{ prime of } L\}$$

is a conj. class of G.

Thm 2.2 (Chebotarev density theorem)

For any conj. cl. C,

$$\mathbb{P}_{\mathfrak{p} \text{ prime of } K \text{ (unram.)}}(\mathrm{Frob}(\mathfrak{p}) = C) = \frac{\#C}{\#G}$$

if we order the $\mathfrak{p}$ by $\mathrm{inv}(\mathfrak{p}) := \mathrm{Nm}(\mathfrak{p})$.

{ Informally: pick $\mathfrak{p}$ and then pick a random $\mathfrak{P}|\mathfrak{p}$

$$\mathbb{P}(\mathrm{Frob}(\mathfrak{P}|\mathfrak{p}) = g) = \frac{1}{\#G}.$$

Rmk If $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_n)$, $\mathrm{Gal}(L|K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$,
$(\zeta_n \mapsto \zeta_n^a) \leftrightarrow a$

then $\mathrm{Frob}(p) = (p \bmod n)$, so Thm 2.1 is a special case.

Def ~~Let L/K be an ext. of number field~~
~~Let f ∈ K~~

a) A (sqfree) pol. $f \in K[X]$ of deg. n has *splitting type* $(k_1, \dots, k_r)$ if $f = f_1 \cdots f_r$ for distinct irreducible $f_1, \dots, f_r \in K[X]$ of degrees $k_1, \dots, k_r$.

b) An unram. prime $\mathfrak{q}$ of a number field K has *splitting type* $(k_1, \dots, k_r)$ in a degree n ext. $L|K$ if $\mathfrak{q}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ for distinct primes $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ of inertia degrees $k_1, \dots, k_r$.

Rmk splitting type (n): a) irreducible b) inert
$(1, \dots, 1)$: splits completely

Thm 2.3 Let K be a n.f., $f \in \mathcal{O}_K[X]$ a monic irred. pol, $\alpha \in \overline{K}$ a root of f, $L = K(\alpha)$, $\mathfrak{q}$ a prime of K $\nmid [\mathcal{O}_L : \mathcal{O}_K[\alpha]]$.
Then, $(f \bmod \mathfrak{q}) \in (\mathcal{O}_K/\mathfrak{q})[X]$ has spl. type $(k_1, \dots, k_r)$
iff $\mathfrak{q}$ has spl. type $(k_1, \dots, k_r)$ in L.

Def A permutation $\pi \in S_n$ has *cycle type* $(k_1, \dots, k_r)$ if it consists of cycles of lengths $k_1, \dots, k_r$ (with $k_1 + \dots + k_r = n$).

Exe $(123)(45)(67)(8) \in S_8 \rightsquigarrow (3,2,2,1)$.

Rmk cycle type (n): single n-cycle
$(1, \dots, 1)$: identity

Lemma 2.4 Let $k_1+\dots+k_r=n$ ~~and~~ and let c_i the nr. of times i occurs among $k_1,\dots,k_r$.

$$\mathbb{P}_{\pi\in S_n}(\pi \text{ has cycle type } (k_1,\dots,k_r)) = \prod_{i=1}^{n} \frac{1}{i^{c_i}\cdot c_i!}$$

Ex $\mathbb{P}(\pi \text{ is } n\text{-cycle}) = \frac{1}{n}$, $\mathbb{P}(\pi = id) = \frac{1}{n!}$

Pf The perm. with cycle type $(k_1,\dots,k_r)$ form a conj. cl. of S_n, i.e. an orbit of the conj. action $G \circlearrowright G$.

$$\Rightarrow \mathbb{P}(\dots) = \frac{\#\text{the orbit}}{\#G} = \boxed{\frac{1}{\#\,\mathrm{Stab}}} = \frac{1}{\prod i^{c_i}\cdot c_i!}$$

This will keep coming up!

How many ways to renumber without changing perm.?
can rotate each cycle, $\rightsquigarrow i^{c_i}$
can permute cycles $\rightsquigarrow c_i!$

$\square$

The splitting type of $\mathfrak{p}$ can be determined from $\mathrm{Frob}(\mathfrak{p})$:

Lemma 2.5 Let $M|L|K$ be ~~a~~ n.f., $M|K$ Galois, $n=\deg(L|K)$, $G=\mathrm{Gal}(M|K)$, $H=\mathrm{Gal}(M|L)$.

G acts on G/H (the n-element set) by left mult., so ~~we can~~ interpret el. of G as permutations in S_n.

$\Rightarrow$ splitting type of unram. ~~prime~~ prime $\mathfrak{p}$ of K in L = cycle type of $\mathrm{Frob}(\mathfrak{p})$.
(only depends on conj. cl!)

The Chebotarev density thm then implies:

Thm 2.6 Let $f \in \mathcal{O}_K(x)$ be a monic $\{$irreducible$\}$ pol. of degree n with Galois group $G \hookrightarrow S_n$ (the embedding is given by the action of G on the n roots of f).

$$\mathbb{P}_{\mathfrak{p}}\left(f \bmod \mathfrak{p} \text{ has splitting type } (k_1, \dots, k_r)\right)$$

$$= \mathbb{P}_{\pi \in G}\left(\pi \text{ has } \cancel{\text{splitting}} \text{ cycle type } (k_1, \dots, k_r)\right).$$

Cor 2.7

$$\mathbb{E}_{\mathfrak{p}}(\# \text{ roots of } f \bmod \mathfrak{p}) = 1$$

Pf HW $\square$

3. Random polynomials

3.1. Over finite fields

~~For a random pol.~~

~~fixed q and~~

~~For a fixed finite field $\mathbb{F}_q$ and a random monic pol. $f \in \mathbb{F}_q[X]$ of degree n, one can ask~~

Thm 3.1.1 (Chebotarev's baby sibling)

$$\underbrace{\lim_{q\to\infty} \mathbb{P}_{\substack{f\in\mathbb{F}_q[X]\\ \text{monic}\\ \text{of degree } n}} (f \text{ has splitting type } (k_1, \dots, k_r))}_{\substack{\text{One can certainly compute this,}\\ \text{but the answer gets cleaner}\\ \text{in the limit } q\to\infty}}$$

$$= \mathbb{P}_{\pi\in S_n} (\pi \text{ has cycle type } (k_1, \dots, k_r))$$

[We first show two examples:]

Exe A $\lim \mathbb{P}$ (f splits completely) $= \frac{1}{n!}$

Pf of Exe s.c.: $f(X) = (X-a_1)\cdots(X-a_n)$ with $a_1, \dots, a_n \in \mathbb{F}_q$

$$\mathbb{P}(\dots) = \frac{\binom{q}{n}}{q^n} = \underbrace{\frac{q}{q}\cdot\frac{q-1}{q}\cdots\frac{q-n+1}{q}}_{\xrightarrow{q\to\infty}\ 1} \cdot \frac{1}{n!}$$

$\square$

Ese[B] $\lim \mathbb{P}(f \text{ irreducible}) = \frac{1}{n}$

Pf of Ese: Let $I_n := \{\text{irred. monic deg } n \text{ pol}\}$

Any $\alpha \in \mathbb{F}_{q^n}$ generates a subfield $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n}$ (with $d \mid n$).

Its min. pol. has degree d.

$\Rightarrow$ We get a map $\mathbb{F}_{q^n} \xrightarrow{\text{min. pol.}} \coprod_{d \mid n} I_d$

Any $f \in I_d$ has exactly d ~~roots~~ preimages (= roots in $\mathbb{F}_{q^n}$).

$$\Rightarrow \quad q^n = \sum_{d \mid n} d \cdot \# I_d$$

$$\Rightarrow \quad 1 = \sum_{d \mid n} d \cdot \underbrace{\frac{\# I_d}{q^n}}_{\substack{\to 0 \text{ unless } d = n \\ (\text{because } \# I_d \leq q^d)}} \xrightarrow{q \to \infty} n \cdot \underbrace{\frac{\# I_d}{q^n}}_{\mathbb{P}(\dots)}$$

$\square$

Rmk: $n \cdot \# I_n = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \cdot q^d$ by Möbius inversion.

[You can see in those two ese that things are uglier before the limit.]

Pf of Thm ~~$(f_{1,1}\cdots f_{1,c_1})\cdots(f_{n,1}\cdots f_{n,c_n})$ with deg~~

With the notation from Lemma 2.4:

$\mathbb{P}($ splitting type $(k_1,\dots,k_r))$

$$= \frac{1}{q^n}\prod_{l=1}^{n}\binom{\# I_l}{c_l} = \prod_{l=1}^{n}\frac{1}{q^{lc_l}}\binom{\# I_l}{c_l}$$

need to choose c_l irreducible factors of degree l

$n = k_1+\dots+k_r = \sum l c_l$

$$= \prod_l \frac{\# I_l}{q^l}\cdots\frac{\# I_l - c_l+1}{q^l}\cdot\frac{1}{c_l!} \longrightarrow \prod_l \frac{1}{l^{c_l} c_l!}$$

$\frac{\# I_l}{q^l} \to \frac{1}{l}$ by Ex B, $\frac{\# I_l - c_l+1}{q^l} \to \frac{1}{l}$

$\prod_l \frac{1}{l^{c_l} c_l!} = \mathbb{P}($cycle type $(k_1,\dots,k_r))$

□

Cor 3.1.2 $\lim \mathbb{P}(f$ squarefree$) = 1$

Pf $\mathbb{P}($squarefree$) = \sum_{(k_1,\dots,k_r)} \mathbb{P}($splitting type $(k_1,\dots,k_r))$

$$= \sum_{(k_1,\dots,k_r)} \mathbb{P}(\text{cycle type } (k_1,\dots,k_r)) = 1$$

□

[Another pf: f sqfree $\Leftrightarrow$ disc$(f)\neq 0$]

Rmk Actually, $\mathbb{P}($squarefree$) = \begin{cases} 1, & n=1 \\ 1-\frac{1}{q}, & n\geq 2\end{cases}$