# Math 286X: Arithmetic Statistics

## Spring 2020

### Problem set #3

**Problem 1.** Let $A \subset \mathbb{R}^n$ be a bounded set whose boundary is Lipschitz. Let $k \geqslant 1$ and $y \in (\mathbb{Z}/k\mathbb{Z})^n$. Show that

$$\lim_{T\to\infty} \mathbb{P}(x \equiv y \mod k \mid x \in (T \cdot A) \cap \mathbb{Z}^n) = \frac{1}{k^n}.$$

**Problem 2.** Find a compact subset $A \subset \mathbb{R}$ with positive volume, but so that

$$\liminf_{T\to\infty} \#((T \cdot A) \cap \mathbb{Z}) = 0.$$

**Problem 3.** Identify the space $V_n$ of monic polynomials of degree $n$ with $\mathbb{R}^n$ by sending $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$ to $(a_{n-1}, \ldots, a_0)$. Consider the map $\varphi_n : \mathbb{R}^n \to V_n \cong \mathbb{R}^n$ sending $x = (x_1, \ldots, x_n)$ to $f(X) = \prod_i (X - x_i)$.

a) Show that the Jacobian determinant at $x \in \mathbb{R}^n$ is $(-1)^n \prod_{i<j}(x_i - x_j)$.

b) Show that the volume of the image $\varphi_3([-1,1]^3) \subset V_3 \cong \mathbb{R}^3$ is $16/45$. (Use a computer if you like.)

**Problem 4.** Fix some $n \geqslant 2$. Order the algebraic integers $\alpha \in \overline{\mathbb{Z}}$ of degree $n$ and trace 0 by length $|\alpha|$. Let $\operatorname{disc}(\alpha)$ be the discriminant of the ring $\mathbb{Z}[\alpha]$. We always have $|\operatorname{disc}(\alpha)| \ll_n |\alpha|^{n(n-1)}$. Show that

$$\lim_{\varepsilon\to 0} \mathbb{P}(|\operatorname{disc}(\alpha)| \geqslant \varepsilon|\alpha|^{n(n-1)} \mid \alpha \text{ as above}) = 1.$$

**Problem 5.** Fix some $n \geqslant 2$. Order the algebraic integers $\alpha \in \overline{\mathbb{Z}}$ of degree $n$ and trace 0 by length $|\alpha|$. Let $\lambda_1(\alpha) \leqslant \cdots \leqslant \lambda_n(\alpha)$ be the successive minima of the lattice $\mathbb{Z}[\alpha] \subset \mathbb{R}^n$ (with respect to the Euclidean norm on $\mathbb{R}^n$, say). We know that $\lambda_1(\alpha) \asymp_n 1$. Since $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent, it is also clear that $\lambda_i(\alpha) \ll_n |\alpha|^i$ for $i = 1, \ldots, n-1$. Show that

$$\lim_{\varepsilon\to 0} \mathbb{P}_{\inf}(\lambda_i(\alpha) \geqslant \varepsilon|\alpha|^i \text{ for } i = 1, \ldots, n-1 \mid \alpha \text{ as above}) = 1.$$

(In particular, assuming $\varepsilon$ is small enough, for a positive proportion of $\alpha$, we have $\lambda_i(\alpha) \geqslant \varepsilon|\alpha|^i$ for $i = 1, \ldots, n-1$. — "The lattice $\mathbb{Z}[\alpha]$ is almost never balanced.")

**Problem 6** (completely unnecessary for us). a) Show that if a monic polynomial $f(X) = X^3 + a_2X^2 + a_1X + a_0 \in \mathbb{R}[X]$ has a root $x \in \mathbb{C}$ with $|x| = 1$, then

$$1 + a_2 + a_1 + a_0 = 0$$

or

$$-1 + a_2 - a_1 + a_0 = 0$$

or

$$a_2a_0 - a_0^2 - a_1 + 1 = 0.$$

b) (if you know algebraic geometry or resultants) Show that for any $n \geqslant 1$, there is a nonzero polynomial $C(A_{n-1}, \dots, A_0) \in \mathbb{Z}[A_{n-1}, \dots, A_0]$ such that for any monic polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{R}[X]$, which has a root $x \in \mathbb{C}$ with $|x| = 1$, we have $C(a_{n-1}, \dots, a_0) = 0$. (And how would you compute such a polynomial $C$?)

**Problem 7.** An isomorphism of graphs $G = (V, E)$ and $G' = (V', E')$ is a bijection $f : V \to V'$ between the sets of vertices such that $(x, y) \in E$ if and only if $(f(x), f(y)) \in E'$. Consider the set of undirected graphs $G$ with $n$ vertices (without loops, i.e., without edges of the form $(x, x)$), up to isomorphism. Show that

$$\sum_G \frac{1}{\# \operatorname{Aut}(G)} = \frac{2^{n(n-1)/2}}{n!}.$$