Math 286X: Arithmetic Statistics

Spring 2020

Problem set #4

Problem 1 (Compare with problem 2 on problem set 3)**.** Let $A \subset \mathbb{R}$ be a compact subset and let $I \subset \mathbb{R}$ be a bounded interval. Let $B \subset \mathbb{R}$ be the weighted set whose characteristic function is the convolution

$$\chi_B(x) = \frac{1}{\mathrm{vol}(I)} \cdot \int_{\mathbb{R}} \chi_A(x-s)\chi_I(s)\mathrm{d}s = \frac{1}{\mathrm{vol}(I)} \cdot \int_{\mathbb{R}} \chi_A(s)\chi_I(x-s)\mathrm{d}s.$$

Show that

$$\#((T \cdot B) \cap \mathbb{Z}) \sim_{A,I} \mathrm{vol}(A) \cdot T$$

for $T \to \infty$.

Solution. We have

$$\begin{aligned}
&\#((T \cdot B) \cap \mathbb{Z}) \\
&= \sum_{x \in \mathbb{Z}} \chi_{T \cdot B}(x) \\
&= \sum_{x \in \mathbb{Z}} \chi_B\left(\frac{x}{T}\right) \\
&= \sum_{x \in \mathbb{Z}} \frac{1}{\mathrm{vol}(I)} \cdot \int_{\mathbb{R}} \chi_A(s)\chi_I\left(\frac{x}{T} - s\right)\mathrm{d}s \\
&= \frac{1}{\mathrm{vol}(I)} \cdot \int_{\mathbb{R}} \chi_A(s) \sum_{x \in \mathbb{Z}} \chi_I\left(\frac{x}{T} - s\right)\mathrm{d}s \\
&= \frac{1}{\mathrm{vol}(I)} \cdot \int_{\mathbb{R}} \chi_A(s) \sum_{x \in \mathbb{Z}} \chi_{T \cdot (I+s)}(x)\mathrm{d}s \\
&= \frac{1}{\mathrm{vol}(I)} \cdot \int_{\mathbb{R}} \chi_A(s)\#((T \cdot (I+s)) \cap \mathbb{Z})\mathrm{d}s \\
&= \frac{1}{\mathrm{vol}(I)} \cdot \int_{\mathbb{R}} \chi_A(s)(\mathrm{vol}(T \cdot (I+s)) + \mathcal{O}(1))\mathrm{d}s \\
&= \frac{1}{\mathrm{vol}(I)} \cdot \int_{\mathbb{R}} \chi_A(s)(\mathrm{vol}(I) \cdot T + \mathcal{O}(1))\mathrm{d}s \\
&= \mathrm{vol}(A) \cdot T + \mathcal{O}\left(\frac{\mathrm{vol}(A)}{\mathrm{vol}(I)}\right).
\end{aligned}$$

□

Problem 2. Explicitly describe fundamental domains for the following actions:

a) The action of $\mathbb{Z}_p$ on $\mathbb{Q}_p$ by translation.

Solution. For example, the set of quotients r/p^e, where $0 \leqslant r < p^e$ and $e \geqslant 0$. (These are the p-adic rational numbers that have only zeroes before the decimal point.) □

b) The action of $\mathbb{Z}_{(p)} = \{p^a b \mid a, b \in \mathbb{Z}\} \subset \mathbb{Q}$ on $\mathbb{R} \times \mathbb{Q}_p$ given by $g.(x, y) = (g + x, g + y)$.

Solution. For example, $[0, 1) \times \mathbb{Z}_p$. □

Problem 3. Let $\mathcal{V}(\mathbb{Z})$ be the set of quadratic forms $aX^2 + bXY + cY^2$ with $a, b, c \in \mathbb{Z}$, ordered by $\max(|a|, |b|, |c|)$. Let p be a prime number. Call an integer $D \in \mathbb{Z}$ *fundamental at p* if $p^2 \nmid D$ when $p \neq 2$ and if $D \equiv 1 \mod 4$ or $D \equiv 8, 12 \mod 16$ when $p = 2$. (This means that $D \neq 1$ is a fundamental discriminant if and only if it is fundamental at every prime p.) Show that

$$\mathbb{P}(\operatorname{disc}(f) \text{ is fundamental at } p \mid f \in \mathcal{V}(\mathbb{Z})) = 1 - p^{-2} - p^{-3} + p^{-4}.$$

(Feel free to use a computer.)

Solution. Let us first handle the case $p \neq 2$. We need to find the probability that $b^2 - 4ac \not\equiv 0 \mod p^2$ for $a, b, c \in \mathbb{Z}/p^2\mathbb{Z}$.

$$\begin{aligned} &\mathbb{P}(b^2 - 4ac \not\equiv 0 \mod p^2 \mid a, b, c \in \mathbb{Z}/p^2\mathbb{Z}) \\ &= 1 - \mathbb{P}(b^2 - 4ac \equiv 0 \mod p^2 \mid a, b, c \in \mathbb{Z}/p^2\mathbb{Z}). \end{aligned}$$

With probability $1 - p^{-1}$, a is not divisible by p. In this case, for any given b, there is exactly one residue class $c \bmod p^2$ so that $b^2 - 4ac \equiv 0 \mod p^2$. Hence, if a is not divisible by p, we have $b^2 - 4ac \equiv 0 \mod p^2$ with probability p^{-2}.

With probability $p^{-1} - p^{-2}$, a is divisible by p exactly once. In this case, we have $b^2 - 4ac \equiv 0 \mod p^2$ if and only if b and c are both divisible by p, which happens with probability p^{-2}.

With probability p^{-2}, a is divisible by p^2. In this case, we have $b^2 - 4ac \equiv 0 \mod p^2$ if and only if b is divisible by p, which happens with probability p^{-1}.

Summing up these probabilities, we obtain

$$\begin{aligned}
&\mathbb{P}(b^2 - 4ac \not\equiv 0 \mod p^2 \mid a, b, c \in \mathbb{Z}/p^2\mathbb{Z}) \\
&= 1 - (1 - p^{-1}) \cdot p^{-2} - (p^{-1} - p^{-2}) \cdot p^{-2} - p^{-2} \cdot p^{-1} \\
&= 1 - p^{-2} - p^{-3} + p^{-4}.
\end{aligned}$$

For $p = 2$, you can either go through an argument similar to the above, or just use a computer to check all $a, b, c \in \mathbb{Z}/16\mathbb{Z}$. □

Problem 4. Let K be a quadratic number field of discriminant D. In class, we've constructed a bijection

$$\mathrm{Cl}_K = K^\times \backslash \{I \text{ fractional ideal of } K\} \longleftrightarrow \mathrm{GL}_2(\mathbb{Z}) \backslash \mathcal{V}_{\mathrm{disc}=D}(\mathbb{Z}).$$

Let $\mathcal{W}(\mathbb{Z}) = \mathcal{V}(\mathbb{Z}) \times \mathbb{Z}^2$ be the set of pairs $e = (f, v)$, where f is a binary quadratic form with integer coefficients, and $v \in \mathbb{Z}^2$. Let $\mathrm{disc}(e) = \mathrm{disc}(f)$ and $\mathrm{Nm}(e) = f(v)$. Furthermore, let $\mathrm{GL}_2(\mathbb{Z})$ act on $\mathcal{W}(\mathbb{Z})$ by $M.(f, v) = (M.f, \det(M)(M^T)^{-1}v)$ (where the action on $\mathcal{V}(\mathbb{Z})$ was defined in class by $(M.f)(w) = f(M^T w)/\det(M)$). For any $N \geqslant 1$, let $\mathcal{W}_{\mathrm{disc}=D, |\mathrm{Nm}|=N} \subset \mathcal{W}$ be the set of $e \in \mathcal{W}$ with $\mathrm{disc}(e) = D$ and $|\mathrm{Nm}(e)| = N$.

a) Construct a bijection

$$\{I \subseteq \mathcal{O}_K \text{ ideal of } \mathcal{O}_K \mid \mathrm{Nm}(I) = N\} \longleftrightarrow \mathrm{GL}_2(\mathbb{Z}) \backslash \mathcal{W}_{\mathrm{disc}=D, |\mathrm{Nm}|=N}(\mathbb{Z}).$$

Solution. Remember that $(1, \tau)$ is a basis of $\mathcal{O}_K$, where $\tau = \frac{D+\sqrt{D}}{2}$.

The group $\mathrm{GL}_2(\mathbb{Q})$ acts freely and transitively on the set of $\mathbb{Q}$-bases (ω_1, ω_2) of K. Let us define an action of $\mathrm{GL}_2(\mathbb{Q})$ on $\mathcal{W}_{\mathrm{disc}=D}(\mathbb{Q})$ exactly in the same way as the action of $\mathrm{GL}_2(\mathbb{Z})$.

To define a $GL_2(\mathbb{Q})$-equivariant map

$$\{(\omega_1, \omega_2) \ \mathbb{Q}\text{-basis of } K\} \longleftrightarrow \mathcal{W}_{\mathrm{disc}=D}(\mathbb{Q}),$$

it then suffices to specify the image $e_0 = (f_0, v_0)$ of the standard basis $(1, \tau)$ of $\mathcal{O}_K$: We use the quadratic form $f_0(X, Y) = X^2 + DXY + \frac{D^2-D}{4}Y^2$ computed in class. To ensure that $|f_0(v_0)| = |\mathrm{Nm}(e_0)| = \mathrm{Nm}(\mathcal{O}_K) = 1$, let's take $v_0 = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$.

If $e = Se_0$ for some matrix $S \in \mathrm{GL}_2(\mathbb{Q})$ with $e = (f, v)$, then

$$\begin{aligned}\mathrm{Nm}(e) &= f(v) = f_0(S^T \det(S)(S^T)^{-1}v_0)/\det(S)\\ &= f_0(\det(S)v_0)/\det(S) = \det(S) \cdot f_0(v_0) = \det(S).\end{aligned}$$

Since the matrix S sends the basis $(1, \tau)$ of $\mathcal{O}_K$ to a basis (ω_1, ω_2) corresponding to e, the norm of the $\mathbb{Z}$-module I generated by ω_1, ω_2 is therefore indeed $|\det(S)| = |\mathrm{Nm}(e)|$.

A short computation shows that the preimage of $e = (f, v) \in \mathcal{W}_{\mathrm{disc}=D}(\mathbb{Z})$ with $f = aX^2 + bXY + cY^2$ and $v = \binom{r}{s}$ is the basis (ω_1, ω_2) with

$$\omega_1 = \left(ar + \frac{b+D}{2} \cdot s\right) - s\tau, \quad \omega_2 = \left(cs + \frac{b-D}{2} \cdot r\right) + r\tau.$$

We've shown in class that the $\mathbb{Z}$-module I generated by ω_1 and ω_2 is a fractional ideal if and only if $a, b, c \in \mathbb{Z}$. It is clear that under this assumption, $I \subseteq \mathcal{O}_K$ (meaning $\omega_1, \omega_2 \in \mathcal{O}_K$) if and only if $r, s \in \mathbb{Z}$ (we have $b - D \equiv b - b^2 \equiv 0 \mod 2$ whenever $a, b, c \in \mathbb{Z}$).

We hence obtain a ($\mathrm{GL}_2(\mathbb{Z})$-equivariant) bijection

$$\{(\omega_1, \omega_2) \text{ basis of } I \subseteq \mathcal{O}_K \mid \mathrm{Nm}(I) = N\} \longleftrightarrow \mathcal{W}_{\mathrm{disc}=D, |\mathrm{Nm}|=N}(\mathbb{Z}).$$

Since $\mathrm{GL}_2(\mathbb{Z})$ acts transitively on the bases of a fixed ideal I, we obtain the desired bijection. □

b) What is the $\mathrm{GL}_2(\mathbb{Z})$-stabilizer of an element of $\mathcal{W}_{\mathrm{disc}=D, |\mathrm{Nm}|=N}(\mathbb{Z})$?

Solution. The stabilizer is trivial, because we have shown above that each element of $\mathcal{W}_{\mathrm{disc}=D, |\mathrm{Nm}|=N}(\mathbb{Q})$ corresponds to only one basis (ω_1, ω_2). □