Math 286X: Arithmetic Statistics

Spring 2020

Problem set #2

Problem 1. Let $L|K$ be a finite Galois extension of number fields with Galois group G. Order the primes $\mathfrak{P}$ of L by $\mathrm{Nm}(\mathfrak{P} \cap K)$. Fix some $g \in G$. Show that

$$\mathbb{P}(\mathrm{Frob}(\mathfrak{P}|\mathfrak{P} \cap K) = g \mid \mathfrak{P} \text{ prime of } L) = \frac{\frac{1}{\mathrm{ord}(g)}}{\sum_{g' \in G} \frac{1}{\mathrm{ord}(g')}}.$$

Solution. Let $C \subseteq G$ be the conjugacy class containing g. For any prime $\mathfrak{p}$ of K whose Frobenius conjugacy class is C, the number of primes $\mathfrak{P}$ lying above it is $[G : D(\mathfrak{p})]$, where $D(\mathfrak{p})$ is the decomposition group of any prime $\mathfrak{P}$ lying above $\mathfrak{p}$. The decomposition group is generated by an element g' of the conjugacy class C, so its index in G is $[G : D(\mathfrak{p})] = \#G/\mathrm{ord}(g') = \#G/\mathrm{ord}(g)$. The number of primes $\mathfrak{P}$ lying above $\mathfrak{p}$ whose Frobenius automorphism is g is therefore $\frac{\#G}{\mathrm{ord}(g)\cdot\#C}$. Hence, for $T \to \infty$

$$\begin{aligned}
&\#\{\mathfrak{P} \mid \mathrm{Frob}(\mathfrak{P}|\mathfrak{P} \cap K) = g \text{ and } \mathrm{Nm}(\mathfrak{P} \cap K) \leqslant T\} \\
&= \#\{\mathfrak{p} \mid \mathrm{Frob}(\mathfrak{p}) = C \text{ and } \mathrm{Nm}(\mathfrak{p}) \leqslant T\} \cdot \frac{\#G}{\mathrm{ord}(g) \cdot \#C} \\
&\sim \#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \leqslant T\} \cdot \frac{\#C}{\#G} \cdot \frac{\#G}{\mathrm{ord}(g) \cdot \#C} \\
&= \#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \leqslant T\} \cdot \frac{1}{\mathrm{ord}(g)}
\end{aligned} \tag{1}$$

by the Chebotarev density theorem. Summing over all $g' \in G$,

$$\begin{aligned}
&\#\{\mathfrak{P} \mid \mathrm{Nm}(\mathfrak{P} \cap K) \leqslant T\} \\
&\sim \#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \leqslant T\} \cdot \sum_{g' \in G} \frac{1}{\mathrm{ord}(g')}.
\end{aligned} \tag{2}$$

Dividing (1) by (2) implies the claim. □

Problem 2. Let Λ be a full lattice in $\mathbb{R}^2$ and let K be a centrally symmetric convex compact subset of $\mathbb{R}^2$. Let the successive minima be $\lambda_1 \leqslant \lambda_2$. Show

that the lattice Λ (not just the vector space $\mathbb{R}^2$) has a basis (l_1, l_2) such that $l_1 \in \lambda_1 K$ and $l_2 \in \lambda_2 K$.
Hint: Use *Pick's theorem*.

Solution. Assume without loss of generality that $\Lambda = \mathbb{Z}^2 \subset \mathbb{R}^2$. Pick any nonzero vector $l_1 \in \mathbb{Z}^2 \cap \lambda_1 K$. Since $\mathbb{Z}^2 \cap \tau K = 0$ for all $0 \leqslant \tau < \lambda_1$, we know that l_1 is a primitive vector in $\mathbb{Z}^2$. Then, pick $l_2 \in \mathbb{Z}^2 \cap \lambda_2 K$ such that the triangle spanned l_1 and l_2 has minimal (nonzero) area. Since the convex set $\lambda_2 K$ contains $0, l_1, l_2$ (and therefore the entire triangle), this means that the triangle cannot contain any lattice points other than the corners 0, l_1, l_2. By Pick's theorem, its area is therefore $\frac{3}{2} - 1 = \frac{1}{2}$. Hence, the area of the parallelogram spanned by l_1 and l_2 (the covolume of the sublattice of $\mathbb{Z}^2$ spanned by l_1 and l_2) is 1, which implies that l_1 and l_2 span $\mathbb{Z}^2$. $\square$

Problem 3. Let K be the smallest centrally symmetric convex subset of $\mathbb{R}^3$ that contains $(1,0,0)$, $(0,1,0)$, and $(1,1,2)$. Let $\lambda_1 \leqslant \lambda_2 \leqslant \lambda_3$ be the successive minima of $\Lambda = \mathbb{Z}^3$. Show that the vectors in $\lambda_3 K \cap \Lambda$ don't generate the lattice Λ (only the vector space $\mathbb{R}^3$).

Solution. Clearly, $\lambda_3 \leqslant 1$, because K contains the linearly independent vectors $(1,0,0)$, $(0,1,0)$, $(1,1,2)$. We will show that $K \cap \mathbb{Z}^3$ generates only the sublattice Λ' of points $(x,y,z) \in \mathbb{Z}^3$ generated by $(1,0,0)$, $(0,1,0)$, $(1,1,2)$, i.e., the set of points such that $2 \mid z$. The set K consists exactly of the points of the form

$$(x,y,z) = \alpha(1,0,0) + \beta(0,1,0) + \gamma(1,1,2) = (\alpha+\gamma, \beta+\gamma, 2\gamma)$$
$$\text{with } |\alpha| + |\beta| + |\gamma| \leqslant 1.$$

Consider a lattice point in K, so

$$\alpha + \gamma \in \mathbb{Z}, \quad \beta + \gamma \in \mathbb{Z}, \quad 2\gamma \in \mathbb{Z}.$$

If $\alpha + \gamma \neq 0$, then $|\alpha| + |\gamma| \geqslant |\alpha + \gamma| \geqslant 1$, implying that $\beta = 0$. Hence, $\gamma \in \mathbb{Z}$ and therefore $\alpha \in \mathbb{Z}$. Indeed, $(x,y,z) \in \Lambda'$. Proceed similarly if $\beta + \gamma \neq 0$. It only remains to consider the case $\alpha + \gamma = \beta + \gamma = 0$, so $\alpha = \beta = -\gamma$. Remember that $1 \geqslant |\alpha| + |\beta| + |\gamma| = 3|\gamma|$. Hence, $2\gamma \in \mathbb{Z}$ can only happen when $\gamma = 0$, and hence $\alpha = \beta = 0$. $\square$

Problem 4. Let $K \subset \mathbb{R}^2$ be the closed disc of radius 1 (with respect to the standard Euclidean length $|\cdot|$ on $\mathbb{R}^2$) and let $\Lambda \subset \mathbb{R}^2$ be any full lattice with successive minima $\lambda_1 \leqslant \lambda_2$. Show that a basis (l_1, l_2) of $\mathbb{R}^2$ is reduced ($|l_1| = \lambda_1$ and $|l_2| = \lambda_2$) if and only if $|l_1| \leqslant |l_2|$ and $|l_1 \cdot l_2| \leqslant \frac{1}{2}|l_1|^2$.

Solution. By definition, $\lambda_1 \leqslant \lambda_2$. Furthermore, as seen in class, if (l_1, l_2) is a reduced basis, then $|l_2 \pm l_1| \geqslant |l_2|$, implying that $|l_1 \cdot l_2| \leqslant \frac{1}{2}|l_1|^2$.

Conversely, assume that (l_1, l_2) is a basis of $\mathbb{R}^2$ such that $|l_1| \leqslant |l_2|$ and $|l_1 \cdot l_2| \leqslant \frac{1}{2}|l_1|^2$. The distance of l_2 from the line spanned by l_1 is then at least $\sqrt{|l_2|^2 - \frac{1}{4}|l_1|^2} \geqslant \frac{\sqrt{3}}{2}|l_2| > \frac{1}{2}|l_2|$. Consider any vector $v = x_1 l_1 + x_2 l_2 \in \Lambda$ $(x_1, x_2 \in \mathbb{Z})$ with $|v| \leqslant |l_2|$. Since the distance of l_2 from the line spanned by l_1 is larger than $\frac{1}{2}|l_2|$, this can only happen if $|x_2| \leqslant 1$. If $x_2 = 0$, we only obtain the multiples of l_1, of which l_1 is of course shortest. Otherwise, assume without loss of generality that $x_2 = 1$. Since $l_1 \cdot l_2 \leqslant \frac{1}{2}|l_1|^2$, one sees that the length of v is minimal for $v = l_2$. Hence, l_1 is shortest among all nonzero vectors in Λ and l_2 is shortest among all vectors in Λ that are not colinear with l_1. □

Let K be a number field of degree n with r_1 real embeddings and r_2 pairs of complex embeddings and with discriminant D_K. We consider the successive minima $1 = \lambda_1 \leqslant \cdots \leqslant \lambda_n$ of $\mathcal{O}_K \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with respect to the norm $|(x_1, \ldots, x_{r_1}, y_1, \ldots, y_{r_2})| = \max(|x_1|, \ldots, |x_{r_1}|, |y_1|, \ldots, |y_{r_2}|)$.

Problem 5. Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ for prime numbers $p < q$.

a) Show that $D_K \asymp p^2 q^2$ and $[\mathcal{O}_K : \mathbb{Z}[\sqrt{p}, \sqrt{q}]] \asymp 1$.

Solution. A convenient $\mathbb{Z}$-basis of $\mathbb{Z}[\sqrt{p}, \sqrt{q}]$ is $\omega_1 = 1$, $\omega_2 = \sqrt{p}$, $\omega_3 = \sqrt{q}$, $\omega_4 = \sqrt{pq}$. The discriminant of $\mathbb{Z}[\sqrt{p}, \sqrt{q}]$ is the determinant of the matrix $(\mathrm{Tr}_{K|\mathbb{Q}}(\omega_i \omega_j))_{i,j}$. Because $\mathrm{Tr}(1) = 4$ and $\mathrm{Tr}(\sqrt{p}) = \mathrm{Tr}(\sqrt{q}) = \mathrm{Tr}(\sqrt{pq}) = 0$, this is a diagonal matrix with entries $4, 4p, 4q, 4pq$, so its determinant is $16^2 p^2 q^2$.

By the relative discriminant formula,

$$D_K = D_{\mathbb{Q}(\sqrt{p})}^2 \cdot \mathrm{Nm}_{\mathbb{Q}(\sqrt{p})|\mathbb{Q}}(D_{K|\mathbb{Q}(\sqrt{p})}),$$

which is divisible by p^2 since $D_{\mathbb{Q}(\sqrt{p})}$ is divisible by p.[1] Similarly, D_K has to be divisible by q^2. The result then follows from

$$\mathrm{disc}(\mathbb{Z}[\sqrt{p}, \sqrt{q}]) = [\mathcal{O}_K : \mathbb{Z}[\sqrt{p}, \sqrt{q}]]^2 \cdot \mathrm{disc}(\mathcal{O}_K).$$ □

b) Show that $\lambda_2 \asymp \sqrt{p}$ and $\lambda_3 \asymp \sqrt{q}$ and $\lambda_4 \asymp \sqrt{pq}$.

[1]For this problem, it would in fact suffice to instead argue that D_K is divisible by p because p is ramified because it is already ramified in $\mathbb{Q}(\sqrt{p})$.

Solution. Since $1, \sqrt{p}, \sqrt{q}, \sqrt{pq}$ are linearly independent elements of $\mathcal{O}_K$ with $|1| < |\sqrt{p}| < |\sqrt{q}| < |\sqrt{pq}|$, we clearly have $\lambda_1 = 1$, $\lambda_2 \ll \sqrt{p}$, $\lambda_3 \ll \sqrt{q}$, $\lambda_4 \ll \sqrt{pq}$. On the other hand, by Minkowski's second theorem,

$$pq \asymp D_K^{1/2} \asymp \lambda_1\lambda_2\lambda_3\lambda_4 \ll 1 \cdot \sqrt{p} \cdot \sqrt{q} \cdot \sqrt{pq} = pq,$$

so the asymptotic inequalities ($\ll$) must in fact be asymptotic equalities ($\asymp$). $\square$

Problem 6 ([Cou19, section 2])**.** We have seen in class that

$$\lambda_i \ll_n |D_K|^{1/(2(n-i+1))} \qquad \text{for } i = 2, \dots, n.$$

In particular,

$$\lambda_n \ll_n |D_K|^{1/2}.$$

Show that in fact

$$\lambda_n \ll_n |D_K|^{1/(\lceil n/2 \rceil + 1)}.$$

Hint: Let $l_1, \dots, l_n$ be a reduced basis of $\mathbb{R}^n$, with $|l_i| = \lambda_i$. Let $r > n/2$. Prove that the integers $l_i l_j$ with $1 \leqslant i, j \leqslant r$ together generate K as a $\mathbb{Q}$-vector space.
Hint 2: Otherwise the r-dimensional space spanned by $l_1, \dots, l_r$ would be perpendicular to itself with respect to some nondegenerate symmetric bilinear form on K.

Solution. Assume that the integers $l_i l_j$ with $1 \leqslant i, j \leqslant r$ do not generate the vector space K. This means that there is a nonzero linear map $f : K \to \mathbb{Q}$ such that $f(l_i l_j) = 0$ for all $1 \leqslant i, j \leqslant r$. The bilinear symmetric form $q : K \times K \to \mathbb{Q}$, $q(x, y) = f(xy)$ is nondegenerate: For any $x \in K$, we have $q(x, K) = f(xK) = f(K) \neq 0$. On the other hand, $q(l_i, l_j) = 0$ for all $1 \leqslant i, j \leqslant r$. The dimension of a subspace and its orthogonal complement with respect to a nondegenerate bilinear form add up to the dimension of the ambient space. In our case, $r + r \leqslant n$, contradicting the assumption that $r > n/2$. Hence, the integers $l_i l_j$ with $1 \leqslant i, j \leqslant r$ indeed generate the vector space K. In particular, by definition $\lambda_n \leqslant \max_{1 \leqslant i,j \leqslant r} |l_i l_j| \leqslant \max_{1 \leqslant i,j \leqslant r} |l_i| \cdot |l_j| = \lambda_r^2$. Then, $|D_K|^{1/2} \asymp_n \lambda_2 \cdots \lambda_n \geqslant \lambda_n^{(n-r)/2+1}$, so $\lambda_n \ll_n |D_K|^{1/(n-r+2)}$. The result follows by choosing $r = \lfloor n/2 \rfloor + 1$. $\square$

References

[Cou19] Jean-Marc Couveignes. *Enumerating number fields*. 2019. arXiv: 1907.13617 [math.NT].