

# 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  $\text{Nm}(\mathfrak{P} \cap K)$ . Fix some  $g \in G$ . Show that

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

**Problem 2.** Let  $\Lambda$  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  $\lambda_1 \leq \lambda_2$ . Show that the lattice  $\Lambda$  (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*.

**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  $\lambda_1 \leq \lambda_2 \leq \lambda_3$  be the successive minima of  $\Lambda = \mathbb{Z}^3$ . Show that the vectors in  $\lambda_3 K \cap \Lambda$  don't generate the lattice  $\Lambda$  (only the vector space  $\mathbb{R}^3$ ).

**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  $\lambda_1 \leq \lambda_2$ . 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  $|l_1| \leq |l_2|$  and  $|l_1 \cdot l_2| \leq \frac{1}{2}|l_1|^2$ .

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  $1 = \lambda_1 \leq \dots \leq \lambda_n$  of  $\mathcal{O}_K \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$  with respect to the norm  $|(x_1, \dots, x_{r_1}, y_1, \dots, y_{r_2})| = \max(|x_1|, \dots, |x_{r_1}|, |y_1|, \dots, |y_{r_2}|)$ .

**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  $[\mathcal{O}_K : \mathbb{Z}[\sqrt{p}, \sqrt{q}]] \asymp 1$ .

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

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

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

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  $1 \leq i, j \leq r$  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  $K$ .

## References

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