Arithmetic Statistics: Exercises

Christopher Keyes

Updated March 11, 2025

Instructions

After each lecture, this document will be updated with appropriate exercises. Exercises may be moved or added as the course goes on, so please check the updated sheet before starting in on the problems.

Expectations

Attempt and hand in **at least 3 problems** of problems on each sheet. You do not have to hand in all the exercises, nor should you feel limited by 3 problems if you want to do more. Some of the problems work out background material; in general, *I encourage you to challenge yourself by choosing exercises that you have not done before.*

Writing your own exercises

If you think of a good problem that isn't already on the sheet, **write it down, along with your solution, and share it with me!** This counts towards one of your 3 problems. Here are some potential sources of good problems.

- I mention something in class without adequate proof, so you work it out.
- You/someone has a question in class and we don't carefully go over the answer.
- You find and work out an example that reinforces your understanding of an idea.
- You come across an exercise in a related book/paper/notes and give it a try.

Coming up with "good" exercises is a skill in itself. Practicing this skill will be useful to you as a researcher when you need to assess your own understanding, and/or as a teacher when working with your own students.

1 Problem sheet 1

Exercise 1.1 (Prime number races)**.** Write some Sage code (or whatever programming language you like) to run a few more "prime number races." Do you notice any patterns? Some features to keep an eye on are the "winners" of the race, as well as the number of "overtakes," i.e. when primes in one residue class become more common than the other(s).

Exercise 1.2 (Prime number races in quadratic fields)**.** Write some Sage code (or whatever programming language you like) to run a different kind of prime number race: for a quadratic field $K/\mathbb{Q}$, compare the counts of primes p which are split in K versus inert in K. How often are the split primes ahead in the race? Try this for several different quadratic fields K. What patterns do you notice?

Hint: here are some potentially useful Sage commands:

- `K = QuadraticField(D)` makes a quadratic field $K = \mathbb{Q}(\sqrt{D})$.
- `K.primes_above(p)` gives a list of prime ideals above p.

Exercise 1.3 (Infinitude of number fields)**.** Prove that for any degree $d > 1$, there are infinitely many number fields $K/\mathbb{Q}$ of degree d.

If you're looking for more of a challenge, prove this for K/F (what properties does F need to satisfy?) and/or add Galois group restrictions.

Exercise 1.4. Let $A_n \subset S_n$ be the alternating group inside the symmetric group on n letters. Suppose $K/\mathbb{Q}$ is a degree n extension. Prove that if $\mathrm{Disc}(K/\mathbb{Q})$ is a square, then $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \subseteq A_n$.

Exercise 1.5. Let $K/\mathbb{Q}$ be an S_3-cubic and $\widetilde{K}/\mathbb{Q}$ its Galois closure, so $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \simeq S_3$.

(a) What are the possible splitting types for an unramified prime p in $\widetilde{K}$?

(b) Match up each splitting type to its conjugacy class in S_3.

(c) Are there any inert primes in $\widetilde{K}$?

Exercise 1.6. Prove that the Chebotarev Density Theorem implies Dirichlet's Theorem on primes in arithmetic progressions, i.e. $\pi(X; a, b) \sim \frac{1}{\varphi(b)} X$.

(*Hint:* cyclotomic extensions.)

Exercise 1.7 (Genus theory)**.** Let D be squarefree and $K = \mathbb{Q}(\sqrt{D})$ be a quadratic extension. Prove that there exists a subgroup

$$(\mathbb{Z}/2\mathbb{Z})^{\omega(D)-1} \subset \mathrm{Cl}(K),$$

where $\omega(D)$ denotes the number of prime divisors of D.

(*Hint:* ramified primes)

Exercise 1.8. Let G be a graph on n *labeled* vertices. The group of automorphisms $\mathrm{Aut}(G) \subseteq S_n$ consists of those permutations of vertices whose induced map on the edge set is an isomorphism. (Note: the labeling of vertices is important here!)

For $n = 3, 4$, write down the 2^n graphs on n labeled vertices and determine their automorphism groups. Now compare the isomorphism class of each graph with its automorphism group — what do you notice? Using $1/\#\,\mathrm{Aut}(G)$ as a weighting, what is the average number of edges for a random graph on n vertices?

2 Problem sheet 2

Exercise 2.1. In the notes, we saw that when counting squarefree numbers in residue classes mod p^2, we have

$$\mathrm{SF}(X; a, p^2) \sim \frac{X}{(p^2-1)\zeta(2)}.$$

Generalize this for an arbitrary modulus N in place of p^2.

Exercise 2.2. For k a positive integer, let $\mathrm{PF}_k(X) = \#\{1 \leq n \leq X : n \text{ is } k\text{-th power free}\}$. Prove that

$$\mathrm{PF}_k(X) = \frac{X}{\zeta(k)} + o(X).$$

What is the smallest power of X you can get in the error term?

Exercise 2.3 (counting quadratic fields by local behavior)**.** Fix a prime, say $p = 5$ for concreteness. Count the number of quadratic extensions $K/\mathbb{Q}$ by discriminant for which

(a) 5 is a split prime in K,

(b) 5 is an inert prime in K,

(c) 5 is ramified in K.

How would you generalize to splitting conditions at *multiple* primes?

(*Hint:* think about how we counted squarefree numbers in congruence classes.)

Exercise 2.4. Carefully prove that the discriminant is a complete isomorphism invariant for quadratic rings. That is, prove Proposition 3.5.

Exercise 2.5. What are the discriminants associated to the quadratic rings $\mathbb{Z} + \mathbb{Z}$ and $\mathbb{Z}[x]/(x^2)$?

Exercise 2.6. Let $D \equiv 0$ or $1 \pmod 4$ and R_D be the quadratic ring of discriminant D. Prove Lemma 3.6; that is, characterize those D for which R_D is an integral domain, and for which R_D is maximal.

Exercise 2.7 (Polynomial discriminants)**.** Try this one if you haven't done it before! Prove that $b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$ is the discriminant of a cubic polynomial $ax^3 + bx^2 + cx + d$. Convince yourself this is tedious but straightforward, possibly by writing a computer program to derive the discriminant formula for a degree n polynomial. Then prove that the discriminant is 0 or 1 modulo 4.

Exercise 2.8 (Cubic rings and cubic forms)**.** Check some of the details in the proof of Proposition 3.7. In particular, perform the "explicit calculation" to see

$$\phi(x\omega + y\theta) = f(x, y)(\omega \wedge \theta)$$

and do the change of basis calculation alluded to in the notes. If it's not clear, flesh out the construction R given a binary cubic form f.

3 Problem sheet 3

Exercise 3.1 (Discriminant of cubic ring)**.** Let R_f be the cubic ring constructed from a binary cubic form. Compute

$$\mathrm{Disc}(R_f) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

(*Hint*: compute the traces of ω, θ first by finding a cubic polynomial they satisfy.)

Exercise 3.2. Find two rank n rings R, R' which are not isomorphic but have the same discriminant. (You will need $n \geq 3$.)

Exercise 3.3. What are the possible automorphism groups for a cubic ring R? Give examples of each. Which automorphism groups can occur for $R = \mathcal{O}_K$ the ring of integers in a cubic field $K/\mathbb{Q}$?

Exercise 3.4. Argue that a rank n ring R is maximal if and only if it can be written

$$R = \prod_{i=1}^{r} \mathcal{O}_{K_i}, \text{ for number fields } K_i \text{ with } \sum_{i=1}^{r} [K_i : \mathbb{Q}] = n.$$

Use this to argue that R is maximal if and only if it is maximal at p for all primes p.

Exercise 3.5 (Hessians)**.** Prove that for f a cubic form and $M \in \mathrm{GL}_2(\mathbb{Z})$, then $H_{M\cdot f} = M \cdot H_f$.

Exercise 3.6 (Quadratic resolvents)**.** Let R be a cubic ring that is an order in a cubic field K.

(a) Prove that $\mathrm{Disc}(R) \mid \mathrm{Disc}(x)$. (*Hint*: argue that $\mathrm{Disc}(x) = \mathrm{Disc}(\mathbb{Z}[x, x^2])$, and then adapt Remark 3.11.)

(b) Prove the map $R \to S$ sending $x \mapsto (\mathrm{Disc}(x) + \sqrt{\mathrm{Disc}(x)})/2$ is well defined.

(c) Prove that $\mathrm{Disc}(x) = \mathrm{Disc}(f(x))$.

(d) Show that f descends to a map $R/\mathbb{Z} \to S/\mathbb{Z} \simeq \mathbb{Z}$. Then show that this map describes the same cubic form as in Proposition 3.7.

Exercise 3.7 (Local densities of quadratic forms)**.** Double check the computations of $\mu_p(T_p(1^2)), \mu_p(T_p(11))$, and $\mu_p(T_p(2))$ from the notes.

How would these change if we instead ask for the subset of p-adic forms with each factorization type over $\mathbb{Z}_p$ rather than modulo p? That is, what happens if we choose not to discard those forms which reduce to zero mod p?

Exercise 3.8 (Local densities of degree n polynomials)**.** There are some interesting papers that prove things about *how often* (in the sense of μ_p-density) p-adic polynomials of degree n have certain properties like having roots, or certain factorization types, etc. More generally, one can ask about local solubility in families of varieties. If you think this sounds like fun, have a look at the paper of Bhargava, Cremona, and Fisher on ternary cubics, [BCF16a], their paper with Jones and Keating on quadratic forms [BCF+16b], or their paper with Gajovic [BCFG22]. If these papers inspire you to solve a explicit local solubility problem of your own, have a go at it!

4 Problem sheet 4

Exercise 4.1. Prove that for any $g \in \mathrm{GL}_2(\mathbb{R})$, we have a unique decomposition $g = kan\lambda$ for $k \in K_1,\ a \in A_+,\ n \in N,\ \lambda \in \Lambda$.

(*Hint*: Gram–Schmidt)

Exercise 4.2 (Haar measure on $\mathrm{GL}_2(\mathbb{R})$)**.** test

(a) Show that $\frac{1}{\lambda} d\lambda$ is a Haar measure on $\mathbb{G}_m(\mathbb{R})$.

(b) Show that $\frac{1}{t^3} dndtdk$ is a Haar measure on $\mathrm{SL}_2(\mathbb{R})$, where N, A, K are the usual subgroups.

Exercise 4.3. Let N', A', K, Λ be as in the definition of $\mathcal{F}$. Fix some real cubic form $v \in V_{\mathbb{R}}$ and compute $nv,\ av,\ kv,\ \lambda v$, in terms of $\mathrm{Disc}(v)$, for $n \in N',\ a \in A',\ k \in K', \lambda \in \Lambda$.

Exercise 4.4. Prove there are $O(X^{3/4+\epsilon})$ cubic forms f in $\mathcal{F}v$ with discriminant less than X and automorphism group C_3. Here are some key intermediate steps; see [BST13, Lemma 22].

(a) Argue that it suffices to fix your favorite v.

(b) Argue that if $\mathrm{Aut}(R_f)$ is C_3 then the Hessian quadratic form H_f is also stabilized by C_3.

(c) Show that $x^2 + xy + y^2$ is the only such *reduced* quadratic form.

(d) Use this and set $v = x^3 - 3xy^2$ to argue that for fixed (a, b, d), there is at most one c for which (a, b, c, d) has automorphism group C_3, then count.

Exercise 4.5. Show that

$$B(C) = \left\{ v = (a, b, c, d) \in V_{\mathbb{R}} : 3a^2 + b^2 + c^2 + 3d^2 \leq C,\ |\mathrm{Disc}(v)| \geq 1 \right\}.$$

is invariant under the action of $\mathrm{SO}_2(\mathbb{R})$. That is, if $f = ax^3 + bx^2y + cxy^2 + dy^3$ is in $B(C)$, and (a', b', c', d') represent the coefficients of $f(\alpha x + \beta y, \gamma x + \delta y)$ for $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SO}_2(\mathbb{R})$, show $(a', b', c', d') \in B(C)$. This might be easiest with the help some symbolic calculations in your favorite computer algebra software.

Exercise 4.6. Carry out the change of variables computation to go between integrals over $\mathrm{GL}_2(\mathbb{R})$ and $V_{\mathbb{R}}^{\pm}$, i.e. show why $|\mathrm{Disc}(v)|^{-1}$ shows up. Again, a symbolic calculator may be helpful.

Exercise 4.7. Come up with an example of a family of regions $\mathcal{R}$ where the main term of the lattice point count gets absorbed into the error terms coming from Davenport's lemma.

Exercise 4.8. Show that the content of a cubic form f agrees with the content of the corresponding cubic ring R_f.

Exercise 4.9. Prove Lemma 5.14 more carefully than in the notes.

References

[BCF16a] Manjul Bhargava, John Cremona, and Tom Fisher. The proportion of plane cubic curves over $\mathbb{Q}$ that everywhere locally have a point. *Int. J. Number Theory*, 12(4):1077–1092, 2016.

[BCF+16b] Manjul Bhargava, John E. Cremona, Tom Fisher, Nick G. Jones, and Jonathan P. Keating. What is the probability that a random integral quadratic form in n variables has an integral zero? *Int. Math. Res. Not. IMRN*, (12):3828–3848, 2016.

[BCFG22] Manjul Bhargava, John Cremona, Tom Fisher, and Stevan Gajović. The density of polynomials of degree n over $\mathbb{Z}_p$ having exactly r roots in $\mathbb{Q}_p$. *Proceedings of the London Mathematical Society*, 124(5):713–736, May 2022.

[BST13] Manjul Bhargava, Arul Shankar, and Jacob Tsimerman. On the Davenport-Heilbronn theorems and second order terms. *Invent. Math.*, 193(2):439–499, 2013.