Miscellaneous preliminaries on arithmetic geometry

One definition of a **hyperelliptic curve** is a curve C over an algebraically closed field k whose function field K is a degree 2 extension of a purely transcendental extension of k.

1. (a) Show that every hyperelliptic curve is birational to a curve of the form $y^2 = f(x)$ where $f \in k[x]$ is a monic squarefree polynomial.

   (b) Conversely, show that every squarefree $f \in k[x]$ gives rise to a hyperelliptic curve in this way.

   (c) Give an example to show that two distinct monic squarefree $f \in k[x]$ can lead to isomorphic curves.

2. (a) Given a hyperelliptic curve $C : y^2 = f(x)$ as above, let D be the divisor arising from the function x on C. Show that the degree of D is 2 and that $\dim \mathrm{H}^0(C, D) = 2$ if $g > 0$.

   (b) Show that a curve C that has a degree 2 divisor D with $\dim \mathrm{H}^0(C, D) = 2$ is hyperelliptic.

3. Let K be the function field of a curve C over $\mathbb{F}_q$. Show that the degree 0 part of the class group of K is finite.

The following is summarized from [Poonen, §2.4]. Recall that a **closed point** of a scheme X is a point $x \in X$ such that $\{x\}$ is Zariski closed in X. For example, over an algebraically closed field $\overline{k}$, there is a bijection between $X(\overline{k})$ and the closed points of X.

4. Let X be a variety over a field k and let $x \in X$. Prove that x is a closed point if and only if the residue field $\kappa(x)$ is a finite extension of k.

Let X be a variety over the field k. The **degree** of a closed point x on X is $[\kappa(x) : k]$.

5. (a) Let X be the plane conic over $\mathbb{Q}$ cut out by $f(x, y, z) = 3x^2 + 4y^2 + 5z^2$. What is the minimal degree of a closed point on X?

   (b) Let Y be the plane cubic over $\mathbb{Q}$ cut out by $g(x, y, z) = x^3 + y^3 + z^3$. What is the minimal degree of a closed point on X?

6. Let $k = \mathbb{F}_q$ and let $X = \operatorname{Spec} \mathbb{F}_{q^n}$ over k.

   (a) What is $\#X$ (as a set)? Are there any closed points? If so, compute their degrees.

   (b) What is $\#X(\mathbb{F}_{q^n})$?

   (c) Think about why these cardinalities are not the same.

7. More generally, let X be a scheme of finite type over $\mathbb{F}_q$. Let N_d be the number of closed points of degree d on X. Prove that for any $n \geq 1$, we have

$$\sum_{d|n} dN_d = \#X(\mathbb{F}_{q^n}).$$

8. Let $X = \mathbb{A}^1$ over $\mathbb{F}_q$.

   (a) Compute the number N_d of closed points of degree d on X.

   (b) Check that

$$\sum_{d|n} dN_d = \#X(\mathbb{F}_{q^n}).$$

Trace formulas

Many of the questions in this section rely on a basic understanding of or comfort with étale or ℓ-adic cohomology. If you are not familiar with these topics, see, e.g., [Milne] for a refresher.

Let X be a smooth and proper scheme over an algebraically closed field k of characteristic $\neq \ell$. Let $f : X \to X$ be a morphism with isolated fixed points. The **Lefschetz fixed point formula** says that the number of fixed points of f counted with multiplicity (if finite) is the alternating sum of the traces of f acting on the ℓ-adic cohomology:

$$\sum (-1)^i \mathrm{Tr}(f^*; \mathrm{H}^i(X, \mathbb{Q}_l)).$$

9. With X as above, use any method to check that the self-intersection of the diagonal Δ_X in $X \times X$ is the Euler characteristic of X.

10. If T is a non-identity element of $\mathrm{GL}_2(k)$, show that the fixed point scheme of T acting on $\mathbb{P}^1$ has degree 2.

11. Can you generalize the above question to $\mathrm{GL}_n(k)$ acting on $\mathbb{P}^{n-1}$?

12. Let $f : \mathbb{P}^1 \to \mathbb{P}^1$ be an endomorphism of degree $d \geq 2$. How many fixed points, with multiplicity, does f have?

13. Let X be a smooth projective curve of genus ≥ 2 over an algebraically closed field. Use the trace formula to show that $\mathrm{Aut}(X) \to \mathrm{Aut}(\mathrm{Jac}(X))$ is injective.

When k has characteristic p and f is the Frobenius map, the above formula is known as the **Grothendieck-Lefschetz trace formula**.

14. Show that if f is the Frobenius map, each fixed point $x \in X$ has multiplicity one (hint: this is equivalent to showing that the action of $1 - df$ on Ω^1_X is injective — why?).

15. A Brauer-Severi variety over a field k is a variety X such that $X_{\overline{k}}$ is isomorphic to some projective space $\mathbb{P}^n_{\overline{K}}$. Use the trace formula to show that a Brauer-Severi variety over a finite field has a rational point.

Let X be a smooth projective variety of dimension n over $k = \mathbb{F}_q$. One of the earliest applications of the trace formula was to show that the **zeta function of X is rational** (part of the Weil conjectures), though the first proof of this fact was by Dwork using p-adic analysis. Recall that the zeta function of X is defined as

$$Z(X;t) := \exp\left(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}\right),$$

where $N_r = \#X(\mathbb{F}_{q^r})$.

16. Check by hand that the zeta function for $\mathbb{P}^1$ is rational.

17. Assume X and Y are two varieties such that $N_r(X) = N_r(Y)$ for all $r \gg 0$. Show that $Z(X;t) = Z(Y;t)$.

18. Let V be a k-vector space and $\alpha : V \to V$ an endomoprhism. Show by induction that

$$\exp\left(\sum_{r=1}^{\infty} \mathrm{Tr}(\alpha^r; V)\frac{t^r}{r}\right) = \det(1-\alpha t; V)^{-1},$$

as formal power series in t.

19. Use Question 18 and the Grothendieck-Lefschetz trace formula to give a formula for the zeta function of X as a rational function of t.

The rest of the **Weil conjectures**, for X as above, are summarized below:

(i) If E is the self-intersection number $(\Delta_X)^2$ of the diagonal Δ_X of $X \times X$, then the zeta function of X satisfies a **functional equation**:

$$Z\left(X; \frac{1}{q^n t}\right) = \pm q^{nE/2} t^E Z(X;t).$$

(ii) (analogue of **Riemann hypothesis**) The zeta function of X may be written in the form

$$Z(X;t) = \frac{\prod_{i=0}^{n-1} P_{2i+1}(t)}{\prod_{i=0}^{n} P_{2i}(t)},$$

where $P_0(t) = 1-t$; $P_{2n}(t) = 1 - q^n t$; and in general, $P_i(t) = \prod_j (1-\alpha_{ij}t) \in \mathbb{Z}[t]$ with α_{ij} algebraic integers with norm $q^{i/2}$.

(iii) If $B_i := \deg P_i(t)$, then $E = \sum_{i=0}^{2n}(-1)^i B_i$. If X arises from a variety $\widetilde{X}$ over a number ring R by reducing modulo a prime ideal of R, then B_i is equal to the the dimension of the ith Betti (singular) cohomology group for $\widetilde{X}$ considered as a analytic space (i.e., the ith Betti number for $\widetilde{X}$).

20. Verify all the parts of the Weil conjectures for $X = \mathbb{P}^1$ over $k = \mathbb{F}_q$. How about for $\mathbb{P}^n$?

21. Let X be a genus g curve over $k = \mathbb{F}_q$. Use the Weil conjectures to show that the numbers $N_1, N_2, \ldots, N_g$ determine N_r for all $r \geq 1$.

22. Prove the Weil conjectures for elliptic curves over $\mathbb{F}_q$ as follows:

(a) Show that the number of $\mathbb{F}_q$-points of an elliptic curve E is the degree of the isogeny $1 - F$, where $F : E \to E$ is the $\mathbb{F}_q$-linear Frobenius, i.e., the qth-power map on coordinates.

(b) If $F^\vee$ denotes the dual isogeny to F, then show that

$$N_r = q^r - (F^r + (F^\vee)^r) + 1,$$

where $F^r + (F^\vee)^r$ represents the multiplication-by-a isogeny for some integer a. (This can be done in several different ways. See [Hartshorne, Exercise IV.4.16] or [Silverman, §V.2] if you need additional hints.)

(c) Show that

$$Z(E;t) = \frac{(1-Ft)(1-F^\vee t)}{(1-t)(1-qt)} = \frac{(1-at+qt^2)}{(1-t)(1-qt)}.$$

(d) Check that the functional equation holds.

(e) Show the Hasse bound for elliptic curves: $|a| \leq 2\sqrt{q}$.
(Hint: you can use a Cauchy-Schwarz type inequality on degree, which is a positive definite quadratic form, or you can compute this even more directly from the fact that $\deg(b + cF) > 0$ for all $b, c \in \mathbb{Z}$.)

(f) Define α_1 and α_2 such that

$$1 - at + qt^2 = (1-\alpha_1 t)(a - \alpha_2 t).$$

Show that $|a| \leq 2\sqrt{q}$ if and only if $|\alpha_i| = \sqrt{q}$.

(g) Verify part (iii) about Betti numbers directly.

23. Let X be a genus g curve over $k = \mathbb{F}_q$. Use the Weil conjectures for the following:

(a) Check that the only nonzero Betti numbers for X are $B_0 = 1$, $B_1 = 2g$, and $B_2 = 1$.

(b) Show that Frobenius acts by the identity on $\mathrm{H}^0(X, \mathbb{Q}_\ell)$ and by multiplication by q on $\mathrm{H}^2(X, \mathbb{Q}_\ell)$.

(c) Show that the absolute value of the trace of Frobenius acting on $\mathrm{H}^1(X, \mathbb{Q}_\ell)$ is $\leq 2g\sqrt{q}$.

(d) Conclude that $|q + 1 - X(\mathbb{F}_q)| \leq 2g\sqrt{q}$.

24. Use the estimate from Question **23** to show that every genus one curve over a finite field has a rational point.

The Weil conjectures can be strengthened to apply to **quasiprojective varieties**, by using compactly supported cohomology. In (ii), one obtains that all eigenvalues on H^i_c have absolute value $\leq q^{i/2}$ for all embeddings.

25. (A generalization of Question **15**) Let X be a smooth projective variety over a finite field k. Assume that, over $\overline{k}$, X has a stratification by affine spaces. Show that X has a rational point.

26. Show that every smooth quadric or cubic surface in $\mathbb{P}^3$ over a finite field k has a rational point.

27. Let X be a geometrically irreducible variety of dimension n over $\mathbb{F}_q$. Show that $X(\mathbb{F}_{q^r})$ is non-empty for all $r \gg 0$. (Hint: use the trace formula and the Weil conjectures to show that $\#X(\mathbb{F}_{q^r}) = q^{rn} +$ "lower order terms" in q. Here, "lower order terms" does not have the usual meaning, rather terms whose sum will be of smaller order.)

28. We now extend Question **24** to higher dimensions. Let X be a torsor for an abelian variety A over a finite field $\mathbb{F}_q$.

(a) Show that $A \times X \cong X \times X$ via $(a, x) \mapsto (a + x, x)$.

(b) Show that $N_r(A) = N_r(X)$ if $N_r(X) \neq 0$.

(c) Prove that $Z(X; t) = Z(A; t)$ (e.g., using Questions **17** and **27**).

(d) Conclude that X has an $\mathbb{F}_q$-rational point, so $X \cong A$ even over $\mathbb{F}_q$.

(e) Extend the preceding to smooth connected algebraic groups A.

Fulton's trace formula for coherent cohomology says that if X is a proper scheme over $\mathbb{F}_q$, then the trace of Frob_{q^n} on $\mathrm{H}^*(X, \mathcal{O}_X)$ is $\#X(\mathbb{F}_{q^n}) \pmod{p}$.

29. Use Fulton's trace formula to redo Question **15**.

30. (A generalization of Question **26**) Show that every hypersurface of degree d in $\mathbb{P}^n$ over a finite field k has a rational point if $d \leq n$.

31. Let E be a supersingular elliptic curve over $\mathbb{F}_p$. Use Fulton's trace formula and the Weil conjectures for elliptic curves to show that the number $E(\mathbb{F}_p)$ is exactly $1 + p$ for $p \geq 5$.

The following problem needs some a little knowledge of **stacks**.

32. For a groupoid X (viewed as a category with all maps being isomorphisms), define $\pi_0(X)$ as the set of isomorphism classes of objects of X, and for any $x \in \pi_0(X)$, let $\pi_1(X,x) = \mathrm{Aut}(x)$. If $\pi_0(X)$ and $\pi_1(X,x)$ are finite for all $x \in X$, then we define the cardinality

$$\#X := \sum_{x\in\pi_0(X)} \frac{1}{\#\pi_1(X,x)}.$$

Note that dividing by the size of $\mathrm{Aut}(x)$ *in counting problems is a common theme in many of the lectures in the workshop!*

For example, if X is a groupoid with a single object and a group G worth of automorphisms, then $\#X = 1/\#G$. Note that if Y is a stack, then $Y(S)$ is a groupoid for any scheme S.

(a) For a finite group G, let $\mathrm{B}G$ be the stack classifying G-torsors in the étale topology, i.e., $\mathrm{B}G$ is the quotient stack $[\mathrm{pt}/G]$. Show (either directly, or by the trace formula) that $\#\mathrm{B}G(\mathbb{F}_q) = 1$.

In contrast, the groupoid $\mathrm{B}(G(\mathbb{F}_q))$ has cardinality $1/G(\mathbb{F}_q)$.

(b) For any quasi-projective variety X over $\mathbb{F}_q$ with an action of a finite group G, show that $\#[X/G](\mathbb{F}_q) = \#(X/G)(\mathbb{F}_q)$, i.e., passage to the coarse moduli space X/G loses no information about the number of rational points.

For any quasi-projective variety X, write $\underline{\mathrm{Sym}}^n(X) := [X^n/S_n]$, the symmetric power of X in the sense of Deligne-Mumford stacks; its coarse moduli space is what one usually calls $\mathrm{Sym}^n(X)$.

(c) Let X be a projective variety over $\mathbb{F}_q$. Calculate $\underline{\mathrm{Sym}}^n(X)(\mathbb{F}_q)$ and $\mathrm{Sym}^n(X)(\mathbb{F}_q)$ in terms of the action of Frobenius on $\mathrm{H}^*(X, \mathbb{Q}_\ell)$.

Galois cohomology

See, e.g., [Serre] if you want more problems on Galois cohomology.

Recall that a *profinite group* is a topological group that is the projective limit of finite groups, each with the discrete topology.

33. Show that a topological group is profinite if and only if it is compact, Hausdorff, and totally disconnected.

34. Which of the following is a profinite group (for the natural topology)?

(a) $\mathbb{Z}_p$

(b) $\mathbb{Q}_p$

(c) $\overline{\mathbb{Z}_p}$ (the ring of integers in the algebraic closure of $\mathbb{Q}_p$)

(d) $\mathrm{SL}_n(\mathbb{Z}_p)$

(e) $\prod_{i=1}^{\infty} \mathbb{Z}_p$

(f) $\oplus_{i=1}^{\infty} \mathbb{Z}_p$

(g) $\mathbb{C}[\![t]\!]$

(h) $\mathbb{F}_p[\![t]\!]$

(i) μ_∞ (all roots of unity)

(j) S^1 (the circle)

(k) $\mathrm{Gal}(L/K)$ for a Galois extension L of a field K

(l) for a group G, the projective limit $\hat{G}$ of the finite quotients of G

35. Show that every open subgroup in a profinite group has finite index. Prove the converse or provide a counterexample.

We recall how to compute the cohomology groups $\mathrm{H}^i(G, A)$, where G is a group and A is a G-module. Let $C^i(G, A)$ be the i-cochains $G^i \to A$ (these are continuous functions if G and A have topologies). Then one considers the standard cochain complex:

$$\cdots \to 0 \to 0 \to C^0(G, A) \stackrel{\delta_0}{\to} C^1(G, A) \stackrel{\delta_1}{\to} C^2(G, A) \stackrel{\delta_2}{\to} \cdots .$$

The boundary maps δ_i are defined as follows on elements $f_i \in C^i(G, A)$:

$$\begin{aligned}
(\delta_0 f_0)(g) &= g f_0(\cdot) - f_0(\cdot) \\
(\delta_1 f_1)(g_1, g_2) &= g_1 f_1(g_2) - f_1(g_1 g_2) + f_1(g_1) \\
(\delta_i f_i)(g_1, \ldots, g_i) &= g_1 f(g_2, \ldots, g_i) + \sum_{j=1}^{i} (-1)^j f(g_1, \ldots, g_j g_{j+1}, \ldots, g_i) \\
&\qquad + (-1)^i f(g_1, \ldots, g_{i-1})
\end{aligned}$$

Then one defines $\mathrm{H}^i(G, A)$ as the quotient $\dfrac{\ker\, \delta_i}{\mathrm{im}\ \delta_{i-1}} = \dfrac{\text{“cocycles''}}{\text{“coboundaries''}}$.

36. What is $C^0(G, A)$? What is $\mathrm{H}^0(G, A)$? What is $\mathrm{H}^1(G, A)$ if G acts trivially on A?

37. Assume that G is discrete. Show that $\mathrm{H}^i(G, -)$ is the ith right derived functor of the left exact functor $\mathrm{H}^0(G, -)$.

38. Let $G := \lim G_j$ be a profinite group, with G_j finite groups, and let $A := \mathrm{colim}\ A_j$ with A_j discrete G_j-modules such that the homomorphisms $A_j \to A_k$ are compatible with the maps $G_k \to G_j$. Show that

(a) $C^i(G, A) = \mathrm{colim}\ C^i(G_j, A_j)$ for all $i \geq 0$

(b) $\mathrm{H}^i(G, A) = \mathrm{colim}\ \mathrm{H}^i(G_j, A_j)$ for all $i \geq 0$.

(c) $G = \lim G/H$ and $A = \mathrm{colim}\ A^H$, where H runs over all open normal subgroups of G, and conclude that $\mathrm{H}^i(G, A) = \mathrm{colim}\ \mathrm{H}^i(G/H, A^H)$ for all $i \geq 0$.

Now also assume that A is a $\mathbb{Q}$-vector space.

(d) Show that $\mathrm{H}^i(G, A) = 0$ for $i > 0$.

39. Let G be a profinite group and let V be a finite-dimensional $\mathbb{C}$-vector space. Assume that G acts continuously on V under the Euclidean topology on V. Prove that the image of the map $G \to \mathrm{GL}(V)$ is finite, i.e., G acts continuously on V under the discrete topology on V.

40. Let G be a finite group, M a (discrete) G-module over a field k, and V a k-vector space. Prove the projection formula:

$$\mathrm{H}^i(G, M) \otimes_k V \cong \mathrm{H}^i(G, M \otimes_k V).$$

41. Compute $\mathrm{H}^1(\hat{\mathbb{Z}}, \mathbb{Q})$ when $\hat{\mathbb{Z}}$ is regarded as

(a) a discrete group.

(b) a profinite group.

42. Let $G = \mathbb{Z}/p$ and let k be a field of characteristic p. Consider the category $\underline{G\text{-mod}}$ of finite dimensional k-vector spaces with a continuous action of G, where k has the discrete topology.

(a) Let $R := k[G]$. Show that $R \cong k[t]/(t^p)$, with t corresponding to $g-1$ for a generator $g \in G$.

(b) Show that $\underline{G\text{-mod}}$ identifies with the category $\underline{\mathrm{Mod}_0(R)}$ of finite R-modules.

(c) Show that the functor $\mathrm{H}^i(G, -)$ on $\underline{G\text{-mod}}$ identifies with $\mathrm{Ext}^i_R(k, -)$ on $\underline{\mathrm{Mod}_0(R)}$.

(d) Show that $\mathrm{H}^i(G, k) \neq 0$ for all i, i.e., G has infinite cohomological dimension. (Hint: use that k has an infinite free resolution over R of the form $(\cdots \to R \to R \to R \to R) \cong k$ with the differentials in the complex being t and t^{p-1} alternately.)

(e) For any $A \in \underline{G\text{-mod}}$, construct a canonical isomorphism between $\mathrm{H}^i(G, A)$ and $\mathrm{H}^{i+2}(G, A)$ for $i \geq 1$.

(f) Extend this discussion to $G = \mathbb{Z}/p^n$ using $k[t]/(t^{p^n})$ instead of $k[t]/(t^p)$.

43. Now let $G = \mathbb{Z}_p$ and let k be a field of characteristic p. Again consider the category $\underline{G\text{-mod}}$ of finite dimensional k-vector spaces with a continuous action of G, where k has the discrete topology.

(a) Let $R = k[[G]] := \lim k[\mathbb{Z}/p^n]$. Show that $R \cong k[\![t]\!]$ with t corresponding to $g-1$ for a topological generator $g \in G$.

(b) Show that $\underline{G\text{-mod}}$ identifies with the category $\underline{\mathrm{Mod}_0(R)}$ of finite R-modules supported (set-theoretically) at $t = 0$.

(c) Show that the functor $\mathrm{H}^i(G, -)$ on $\underline{G\text{-mod}}$ identifies with $\mathrm{Ext}^i_R(k, -)$ on $\underline{\mathrm{Mod}_0(R)}$.

(d) Show that $\mathrm{H}^i(G, M) = \mathrm{H}^i(M \to M)$, where the map is $g-1$. In particular, G has cohomological dimension 1.

(e) Recall from Question **38** that $\mathrm{H}^i(G, M) = \mathrm{colim}\, \mathrm{H}^i(\mathbb{Z}/p^n, M^{p^n\mathbb{Z}_p})$. Using Question **42**, analyze these direct limits (to understand why the direct limit is 0 for $i > 1$ even though none of the constituent terms vanishes).

(f) Extend this discussion to $G = (\mathbb{Z}_p)^n$ using $k[\![t_1, ..., t_n]\!]$ instead of $k[\![t]\!]$.

44. Let k be a field of characteristic p and let $n \geq 2$.

(a) Show that $\mathrm{H}^i(\mathbb{Z}/p, k) \neq 0$ for all i.

(b) Let X be a hypersurface of degree $d \leq n$ in $\mathbb{P}^n$ over k. Show that $\mathrm{H}^i(X, \mathcal{O}_X) = 0$ for all $i > 0$.

(c) Show that $\mathbb{Z}/p$ cannot act freely on X.

(Hint: if it does, then compute the cohomology of X/G.)

45. *Additive Hilbert Theorem 90.* Let K be a field, and let L/K be a finite Galois extension with group G. Show that $\mathrm{H}^i(G, L) = 0$ for $i > 0$.

(Hint: formulate a generalization of this statement with L a product of separable field extensions. Check the case of $L = \prod_{g\in G} K$ with the permutation action. Then apply Question **40** with $V = L$, using that $L \otimes_K L \cong \prod_{g\in G} L$ since L/K is Galois.)

46. Let K be a field with a separable closure $\overline{K}$ and absolute Galois group G.

(a) Use Question **45** to show that $\mathrm{H}^i(G, \overline{K}) = 0$ for $i > 0$ and $H^0(G, \overline{K}) = K$.

Assume now that K has characteristic $p > 0$.

(b) Show that the sequence of G-modules

$$1 \to \mathbb{F}_p \to \overline{K} \xrightarrow{\text{Frob}-1} \overline{K} \to 1$$

is exact.

(c) Show that $\mathrm{H}^i(G, \mathbb{F}_p) = 0$ for $i \geq 2$, $\mathrm{H}^1(G, \mathbb{F}_p) = \text{coker}\,(\text{Frob} - 1)$, and $\mathrm{H}^0(G, \mathbb{F}_p) = \mathbb{F}_p$. Use this to conclude that $\widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}}$ cannot be the absolute Galois group of a characteristic p field.

(d) For any $\mathbb{F}_p[G]$-module M, show that $\mathrm{H}^i(G, M) = 0$ for $i > 1$. In particular, the p-cohomological dimension of G is ≤ 1.

(e) Give examples of characteristic p fields K whose ℓ-cohomological dimension is large, where $\ell \neq p$.

Preliminary analytic techniques

Counting lattice points in bounded regions

For a bounded open set $B \subset \mathbb{R}^n$, let $MP(B)$ denote the greatest d-dimensional volume of any projection of B onto a coordinate subspace obtained by equating $n-d$ coordinates to zero, where d takes all values from 1 to $n-1$.

47. **(Davenport's lemma, easy version:)** Let $B \subset \mathbb{R}^n$ be a fixed open bounded set. Assume that B is defined by finitely many polynomial inequalities. Prove that we have

$$\#\{g \cdot B \cap \mathbb{Z}^n\} = \mathrm{Vol}(g \cdot B) + O(MP(g \cdot B)), \tag{1}$$

where $g \in \mathrm{GL}_n(\mathbb{R})$ is any diagonal matrix with positive entries, and the volume of sets in $\mathbb{R}^n$ is normalized so that $\mathbb{Z}^n$ has covolume 1.

Prove the same estimate for $g = nt \in \mathrm{GL}_n(\mathbb{R})$, where n is a lower triangular matrix, and t is a diagonal matrix with increasing positive diagonal entries. Hint: use the fact that only smaller coordinates are being added to larger coordinates.

48. Modify the necessary arguments to obtain an estimate analogous to (1) when $\mathbb{Z}^n$ is replaced with an arbitrary lattice. In particular, when L is a lattice defined by congruence conditions modulo finitely many prime powers $p_1^{k_1}, \ldots, p_m^{k_m}$, prove that we have

$$\#\{g \cdot B \cap \mathbb{Z}^n\} = \mathrm{Vol}(g \cdot B) \prod_{i=1}^{m} \mathrm{Vol}(L_p) + O(MP(g \cdot B)), \tag{2}$$

where L_p is the p-adic closure of L in $\mathbb{Z}_p^n$ and the measure on $\mathbb{Z}_p^n$ is normalized so that $\mathbb{Z}_p^n$ has volume 1.

49. Modify the necessary definitions and arguments to obtain estimates analogous to (1) and (2) when B is an open bounded multiset.

Counting using L-functions

Let $(a_n)_{n \geq 1}$ be a sequence and let

$$L(s) := \sum_{n \geq 1} \frac{a_n}{n^s}$$

be the associated L-function. The next few questions extract information about the partial sums

$$\sum_{n \leq X} a_n$$

from the analytic properties of L.

These questions follow the text of [Elkies, February 8].

50. Prove that for any positive real numbers c and y, we have

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} y^s \frac{ds}{s} = \begin{cases} 1 & \text{if } y > 1; \\ 0 & \text{if } y < 1, \end{cases}$$

in the following sense:

$$\lim_{T\to\infty} \frac{1}{2\pi i}\int_{c-iT}^{c+iT} y^s \frac{ds}{s} = \begin{cases} 1 & \text{if } y > 1; \\ 0 & \text{if } y < 1. \end{cases}$$

51. In fact, prove that

$$\frac{1}{2\pi i}\int_{c-iT}^{c+iT} y^s \frac{ds}{s} = \begin{cases} 1 + O(y^c \min(1, \frac{1}{T|\log y|})) & \text{if } y > 1; \\ O(y^c \min(1, \frac{1}{T|\log y|})) & \text{if } y < 1. \end{cases}$$

52. Conclude that for positive $X \in \mathbb{R} \setminus \mathbb{Z}$ we have

$$\sum_{n\le X} a_n = \frac{1}{2\pi i}\int_{c-iT}^{c+iT} X^s L(s) \frac{ds}{s} + O\Big(\sum_{n=1}^{\infty} a_n \frac{X^c}{n^c} \min\big(1, \frac{1}{T|\log(X/n)|}\big)\Big).$$

53. Use the above estimate to give an (extremely complicated) proof of the fact that the number of positive integers less than X is $X + O(1)$.

An elementary sieve

We compute the "probability" that an integer is squarefree.

54. Let $[X]$ denote the set of positive integers $n \le X$. Let $[X]_{a\,(b)}$ (resp. $[X]^{\text{sf}}$) denote the subset of integers $n \in [X]$ such that $n \equiv a \pmod{b}$ (resp. n is squarefree). Prove the inclusion-exclusion formula

$$\#[X]^{\text{sf}} = \sum_{n=1}^{\infty} \mu(n) \#[X]_{0\,(n^2)}.$$

55. Estimate $\#[X]_{0\,(n^2)}$ for $n \le X^{1/2}$, note that $\#[X]_{0\,(n^2)} = 0$ for $n > X^{1/2}$ and prove that

$$\lim_{X\to\infty} \frac{\#[X]^{\text{sf}}}{\#[X]} = \frac{1}{\zeta(2)}.$$

Of course, the same argument works for negative integers. Thus, with an appropriate definition of probability, we can say that the probability of an integer being squarefree is $1/\zeta(2)$.

56. How many quadratic fields exist having discriminant bounded by X? (Warning: you have to be careful about the conditions on the discriminant modulo 2.)

Proof of Davenport's theorem

Let V denote the space of binary cubic forms, i.e.,

$$V_R := \{ax^3 + bx^2y + cxy^2 + dy^3 : a, b, c, d \in R\},$$

for any ring R. Consider the action of GL_2 on V given by

$$(\gamma \cdot f)(x, y) := \frac{1}{\det \gamma} f((x, y) \cdot \gamma). \tag{3}$$

Let $V_{\mathbb{Z}}^{\mathrm{irr}}$ (resp. $V_{\mathbb{Z}}^{\mathrm{red}}$) denote the set of integral binary cubic forms that are irreducible (resp. reducible). Then **Davenport's Theorem** [Davenport] states the following:

1. The number of $\mathrm{GL}_2(\mathbb{Z})$-orbits on $V_{\mathbb{Z}}^{\mathrm{irr}}$ having positive discriminant bounded by X is $\frac{\pi^2}{72}X + O(X^{5/6})$.
2. The number of $\mathrm{GL}_2(\mathbb{Z})$-orbits on $V_{\mathbb{Z}}^{\mathrm{irr}}$ having negative discriminant with absolute value bounded by X is $\frac{\pi^2}{24}X + O(X^{5/6})$.

Davenport originally obtained an error bound of $O(X^{15/16})$. The improved error bound is due to Bhargava. In the next several problems, we sketch a proof of the above theorem.

57. Check that (3) defines a left action of G on V.

58. Check that the discriminant Δ of the binary cubic form is a relative invariant for the action of G, i.e.,

$$\Delta(\gamma \cdot f) = (\det \gamma)^{\kappa} \Delta(f),$$

where $\gamma \in G$, $f \in V$, and κ is a fixed integer. What is κ equal to?

59. Prove that the set $\{f \in V_{\mathbb{C}} : \Delta(f) \neq 0\}$ consists of one $\mathrm{GL}_2(\mathbb{C})$-orbit. (Hint: Use the fact that $\mathrm{GL}_2(\mathbb{C})$ acts triply transitively on $\mathbb{P}^1_{\mathbb{C}}$.) Prove that the stabilizer in $\mathrm{GL}_2(\mathbb{C})$ of any element in this orbit is isomorphic to S_3. (Hint: You only have to prove this statement for one form f having nonzero discriminant!)

60. Prove that the set $\{f \in V_{\mathbb{R}} : \Delta(f) \neq 0\}$ consists of two $\mathrm{GL}_2(\mathbb{R})$-orbits, namely, the orbit of positive discriminant binary cubic forms and the orbit of negative discriminant binary cubic forms. Denote these two sets by $V_{\mathbb{R}}^{+}$ and $V_{\mathbb{R}}^{-}$, respectively. Prove that the stabilizer in $\mathrm{GL}_2(\mathbb{R})$ of any element in $V_{\mathbb{R}}^{+}$ is isomorphic to S_3, and the stabilizer in $\mathrm{GL}_2(\mathbb{R})$ of any element in $V_{\mathbb{R}}^{-}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

61. Let $\mathcal{F}$ be any fundamental domain for the left action of $\mathrm{GL}_2(\mathbb{Z})$ on $\mathrm{GL}_2(\mathbb{R})$, and let $v^{\pm} \in V_{\mathbb{R}}^{\pm}$ be a fixed vector. We consider $\mathcal{F} \cdot v_{\pm}$ to be a multiset, where the multiplicity of a vector $v \in V_{\mathbb{R}}^{\pm}$ in this multiset is given by $m(v) := \#\{g \in \mathcal{F} : g \cdot v^{\pm} = v\}$. Prove that

$$\sum_{h\in \mathrm{GL}_2(\mathbb{Z})} m(h\cdot v) := \#\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(v),$$

for every $v\in V_{\mathbb{R}}^{\pm}$. Conclude that the $\mathrm{GL}_2(\mathbb{Z})$-orbit of v is represented

$$\#\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(v)/\#\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(v)$$

times in the multiset $\mathcal{F}\cdot v_{\pm}$.

62. For any $\mathrm{GL}_2(\mathbb{Z})$-invariant set $S\subset V_{\mathbb{R}}^{\pm}$, let $N(S;X)$ denote the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits $\mathrm{GL}_2(\mathbb{Z})\cdot v$ in S such that $0<|\Delta(v)|\le X$, where each such orbit is weighted by $1/\#\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(v)$. Conclude from the above problem that we have

$$n^{\pm}N(S;X) = \#\{\mathcal{F}\cdot v^{\pm}\cap S_{|\Delta|\le X}\},$$

where $n^{+}=6$, $n^{-}=2$, $S_{|\Delta|\le X}$ denotes the set of elements $v\in S$ with $0<|\Delta(v)|\le X$, and each element v in the intersection is counted with multiplicity $m(v)$.

63. (**Averaging method of Bhargava** [Bhargava]) Let dg denote any Haar-measure on $\mathrm{GL}_2(\mathbb{R})$. Let G_0 be a fixed nonempty open bounded set in $\mathrm{GL}_2(\mathbb{R})$. It follows from the previous problem that we have

$$n^{\pm}N(S;X) = \frac{\displaystyle\int_{g\in G_0}\#\{\mathcal{F}g\cdot v^{\pm}\cap S_{|\Delta|\le X}\}dg}{\displaystyle\int_{g\in G_0}dg}.$$

(Check this!) Prove that

$$\int_{g\in G_0}\#\{\mathcal{F}g\cdot v^{\pm}\cap S_{|\Delta|\le X}\}dg = \int_{g\in \mathcal{F}}\#\{gG_0\cdot v^{\pm}\cap S_{|\Delta|\le X}\}dg, \tag{4}$$

where again we regard $gG_0\cdot v^{\pm}$ as a multiset, in the following steps:

1. "Unfold" the left hand side of (4) into a sum over $S_{|\Delta|\le X}$, and show that the contribution from each $v\in S_{|\Delta|\le X}$ is equal to

$$\sum_{\substack{h\in \mathrm{GL}_2(\mathbb{R})\\ h\cdot v^{\pm}=v}}\mathrm{Vol}(G_0\cap\mathcal{F}^{-1}h),$$

   where the volume is taken with respect to the Haar-measure dg.

2. Using the unimodularity of the Haar-measure, conclude that

$$\mathrm{Vol}(G_0\cap\mathcal{F}^{-1}h) = \mathrm{Vol}(G_0h^{-1}\cap\mathcal{F}^{-1}) = \int_{g\in\mathcal{F}}\#\{g_0\in G_0 : gg_0 = h\}.$$

3. “Refold” the sum to recover the right hand side of (4).

To estimate $\int_{g\in\mathcal{F}} \#\{gG_0\cdot v^{\pm}\cap S_{|\Delta|\leq X}\}dg$, we will have to construct a convenient fundamental domain $\mathcal{F}$ and choose dg and G_0. For this, we use the Iwasawa decomposition:

64. Consider the subgroups

$$\Lambda = \{\begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} : \lambda > 0\},\ \ N = \{\begin{pmatrix} 1 & \\ n & 1 \end{pmatrix} : n \in \mathbb{R}\},\ \ A = \{\begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} : t > 0\},\ \ K = \mathrm{SO}_2(\mathbb{R}). \tag{5}$$

Prove that the product ΛNAK is equal to $\mathrm{GL}+_2(\mathbb{R})$, the index-2 subgroup of $\mathrm{GL}_2(\mathbb{R})$ consisting of elements having positive determinant.

65. Prove that with these coordinates, the measure

$$dg := d^{\times}\lambda dn \frac{d^{\times}t}{t^2}dk := \frac{d\lambda}{\lambda}dn\frac{dt}{t^3}dk,$$

is a Haar-measure on $\mathrm{GL}_2(\mathbb{R})$. We normalize dk such that K has volume 1.

66. Show that we may pick a fundamental domain $\mathcal{F} := \{nak\lambda : n \in N'(a), a \in A', k \in K, \lambda \in \Lambda\}$ for the left action of $\mathrm{GL}_2(\mathbb{Z})$ on $\mathrm{GL}_2(\mathbb{R})$, where

$$N'(a) = \{\begin{pmatrix} 1 & \\ n & 1 \end{pmatrix} : n \in \nu(a)\},\ \ A' = \{\begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} : t \geq \sqrt[4]{3}/\sqrt{2}\}; \tag{6}$$

here $\nu(a)$ is either equal to $[-\frac{1}{2}, \frac{1}{2}]$ or the union of two subintervals of $[-\frac{1}{2}, \frac{1}{2}]$ depending only on the value of $a \in A'$.

We have picked a fundamental set $\mathcal{F}$ and a Haar measure dg. All we need about the set G_0 is that it is nonempty, open, bounded, and K-invariant.

67. Prove that such a set G_0 exists.

68. Prove the estimate

$$\#\{gG_0 \cdot v^{\pm} \cap V_{\mathbb{Z}}\} = \lambda^4 \mathrm{Vol}(G_0 \cdot v^{\pm}) + O(\lambda^3 t^3),$$

for $g \in \mathcal{F}$ with $g = (\lambda, n, t, k)$.

69. Prove that there exists an absolute constant C such that if $g \in \mathcal{F}$ with $g = (\lambda, n, t, k)$ and $t > C\lambda^{1/3}$, then

$$\#\{gG_0 \cdot v^{\pm} \cap V_{\mathbb{Z}}^{\mathrm{irr}}\} = 0.$$

70. Let $R \subset V_{\mathbb{R}}$ be a set that is contained in a cube with side length T. Then prove that

$$\#\{R \cap V_{\mathbb{Z}}^{\text{red}} = O(T^{3+\epsilon})\}$$

via the following steps:

1. First estimate the number of forms that have x or y as a factor.
2. If $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$, with $a, d \neq 0$ is reducible, then it must have a linear factor $px + qy$ with $p \mid a$ and $q \mid d$. Use this to estimate the number of possible pairs (p,q) once a and d are fixed.
3. Prove that if a, b, d, p, and q are fixed, then c is determined.

71. Modify the above proof to yield a result for sets R that are contained in boxes with possibly different side lengths. As a consequence, obtain a bound for the following quantity:

$$\int_{\substack{g=(\lambda,n,t,k)\in\mathcal{F} \\ \lambda \leq X^{1/4} \\ t < C\lambda^{1/3}}} \#\{gG_0 \cdot v^{\pm} \cap V_{\mathbb{Z}}^{\text{red}}\} dg. \tag{7}$$

72. Using **68**, **69**, and **71**, prove that

$$\int_{g\in\mathcal{F}} \#\{gG_0 \cdot v^{\pm} \cap \{v \in V_{\mathbb{Z}}^{\text{irr}} : |\Delta(v)| \leq X\}\} dg = \int_{g\in\mathcal{F}} \text{Vol}(\{v \in gG_0 \cdot v^{\pm} : |\Delta(v) \leq X\}) dg.$$

73. Using a modification of the argument in **63**, show that

$$\int_{g\in\mathcal{F}} \text{Vol}(\{v \in gG_0 \cdot v^{\pm} : |\Delta(v) \leq X\}) dg = \text{Vol}(\{v \in \mathcal{F} \cdot v^{\pm} : |\Delta(v) < X|\}).$$

74. Denote the set in the right hand side of the above equation by $\mathcal{R}_X$. To compute the volume of $\mathcal{R}_X$, consider the map $\text{GL}_2(\mathbb{R}) \to V_{\mathbb{R}}$ given by $\gamma \mapsto \gamma \cdot v^{\pm}$. Prove the following "change of variables" formula: $dg = |\Delta(v)^{-1}| dv$.

75. Prove Davenport's theorem with the improved error term of $O(X^{5/6})$.

76. Modify the statement of Davenport's theorem, and its proof, to deduce an analogous count of integral irreducible binary cubic forms whose coefficients satisfy a finite set of $\text{GL}_2(\mathbb{Z})$-invariant congruence conditions.

Counting cubic fields

A cubic ring is a commutative ring with unit that is free of rank 3 as a $\mathbb{Z}$-module. A result of Delone and Faddeev [DF] refined by Gan, Gross, and Savin [GGS] states that there is a natural bijection between $\mathrm{GL}_2(\mathbb{Z})$-orbits on $V_{\mathbb{Z}}$ and isomorphism classes of cubic rings. Furthermore, if f is a binary cubic form whose $\mathrm{GL}_2(\mathbb{Z})$-orbit corresponds to the cubic ring R, then the following are true.

1. $\Delta(R) = \Delta(f)$.
2. R is an integral domain if and only if f is irreducible.
3. The splitting of a prime p in R is determined by the factoring of f modulo p.
4. The cubic ring R is nonmaximal at p if and only if f is a multiple of p or there is a $\mathrm{GL}_2(\mathbb{Z})$-translate of f such that p^2 divides the x^3-coefficient and p divides the x^2y-coefficient.

77. Show that a cubic integral domain is maximal if and only if it is maximal at every prime.

78. Compute the probability that a binary cubic form corresponds to a cubic ring maximal at p.

79. Assume that the number of cubic rings having discriminant bounded by X that are nonmaximal at every prime dividing n is bounded by $O(X/n^{2-\epsilon})$. Then use the sieve methods developed in previous questions to prove the Davenport-Heilbronn theorem [DH]:

Theorem: Let $N^{\pm}(X)$ denote the number of cubic fields K such that $0 < \pm\Delta(K) \leq X$. Then we have

$$\begin{aligned} N^{+}(X) &= \frac{X}{12\zeta(3)} + o(X); \\ N^{-}(X) &= \frac{X}{4\zeta(3)} + o(X). \end{aligned} \tag{8}$$

80. By studying how the error term in **76** depends on the modulus of the imposed congruence conditions, improve the $o(X)$ error term above to a power saving.

Galois representations coming from field extensions, and the associated Artin L-functions

Let K be a finite extension of $\mathbb{Q}$ or $\mathbb{Q}_p$. Let G_K denote the absolute Galois group of K, i.e., the group $\mathrm{Gal}(\overline{K}/K)$. A representation of G_K is called a *Galois representation*. In this section, we shall consider Galois representations

$$G_K \to \mathrm{GL}_n(\mathbb{C}),$$

where K is a number field.

Let L/K be a finite Galois extension with Galois group G and let $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ be a representation. Then the representation $G_K \to G \to \mathrm{GL}_n(\mathbb{C})$ is called an Artin representation. We consider the incomplete Artin L-function defined by

$$L^*(s, \rho) := \prod_{\mathfrak{p}} \det[I - N(\mathfrak{p})^{-s}\rho(\mathrm{Frob}(\mathfrak{p}))]^{-1},$$

where the product runs over primes $\mathfrak{p}$ of L that do not ramify. The completed L function is obtained by multiplying L^* with appropriate factors at the ramified primes and the infinite places.

In the questions that follow, all equalities of L-functions are up to a finite number of products (at the ramified primes). Note that this does not affect several analytic properties of the L-functions including meromorphic continuation and the position and multiplicities of its zeroes and poles.

81. Write the Riemann zeta function as an Artin L-function. Write the Dirichlet L-functions as Artin L-functions.

82. Assume that $\rho = \rho_1 \oplus \rho_2$. Then $L^*(s, \rho) = L^*(s, \rho_1)L^*(s, \rho_2)$.

83. Suppose M is an intermediary extension between L and K, normal over K. Denote the Galois group of L/M by H. If ρ is a representation of G/H, then let $\widetilde{\rho}$ denote the natural extension to G. Prove that $L^*(s, \rho) = L^*(s, \widetilde{\rho})$.

84. Suppose M is any intermediary extension between L and K. Denote the Galois group of L/M by H. For a representation ρ of H, let ρ^* denote the induced representation. Then $L(s, \rho^*) = L(s, \rho)$.

85. Let K over $\mathbb{Q}$ be a finite normal extension with Galois group G. Prove that

$$\zeta_K(s) = \prod_{\rho} L^*(s, \rho)^{\dim \rho},$$

where the product ranges over all irreducible representations ρ of G.

86. Assuming that the Dedekind zeta function $\zeta_K(s)$ has a simple pole at 1, and no other poles, prove that $L(1,\chi) \neq 0$ for Dirichlet L-functions $L(s,\chi)$, thus recovering the key step in Dirichlet's proof of the infinitude of primes in arithmetic progressions.

Artin's conjecture states that $L(s,\rho)$ has a meromorphic continuation to the whole complex plane, and is analytic everywhere except for a pole at 1 with multiplicity equal to the multiplicity of the trivial representation in ρ.

87. Prove Artin's conjecture for L-functions arising from S_3-extensions of $\mathbb{Q}$.

88. Let ρ denote the irreducible 2-dimensional extension of S_3. Let K be an S_3-extension of $\mathbb{Q}$, and let $L(s,\rho)$ denote the corresponding L-function. Let K_3 denote one of the three conjugate subfields of K_6 that have degree 3 over $\mathbb{Q}$. Determine the p-th coefficient of $L(s,\rho)$ in terms of the splitting of p in K_3.

89. Write down the list of possible splitting behaviours of a prime p in a cubic S_3-field, and determine the "probability" of each possible splitting type as we range over the family of all cubic fields, ordered by discriminant.

90. Consider the following family of Artin L-functions: let F be the family of all cubic S_3-fields. For each $K \in F$, let $L_K(s) := \zeta_K(s)/\zeta(s)$. Compute the average size of the p-th coefficient of these L-functions.

These computations were done by Andrew Yang in his thesis [Yang], and he used them to determine (assuming GRH) the symmetry type of the low lying zeroes of these L-functions.

References

[BBP] K. Belabas, M. Bhargava, and C. Pomerance, *Error terms for the Davenport-Heilbronn theorems*, Duke Math. J. **153** (2010), 173-210.

[Bhargava] M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. **162**, 1031–1063.

[Davenport] H. Davenport, *On the class-number of binary cubic forms I and II*, J. London Math. Soc. **26** (1951), 183–198.

[DH] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields II*, Proc. Roy. Soc. London Ser. A **322** (1971), no. 1551, 405–420.

[DF] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, AMS Translations of Mathematical Monographs **10**, 1964.

[GGS] W. T. Gan, B. Gross, and G. Savin, *Fourier coefficients of modular forms on G_2*, Duke Math. J. **115** (2002), no. 1, 105169.

[Elkies] N. Elkies, *Lecture notes for Math 229*, `http://www.math.harvard.edu/~elkies/M229.09/index.html`.

[Hartshorne] R. Hartshorne, *Algebraic Geometry*, Springer, 1977.

[Milne] J. S. Milne, *Lectures on Etale Cohomology*, `http://www.jmilne.org/math/CourseNotes/lec.html`.

[Poonen] B. Poonen, *Rational Points on Varieties*, `http://www-math.mit.edu/~poonen/papers/Qpoints.pdf`.

[Serre] J. P. Serre, *Galois Cohomology*, Springer, 1997.

[Silverman] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1986.

[Yang] A. Yang, *Distribution problems associated to zeta functions and invariant theory*, Thesis (Ph.D.)–Princeton University, 2009.