LECTURE NOTES FOR SMS SUMMER SCHOOL "COUNTING ARITHMETIC OBJECTS" JUNE 23–JULY 04, 2014

STANLEY YAO XIAO
stanley.xiao@uwaterloo.ca
Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario, Canada N2L 3G1

AND

JUSTIN SCARFY
scarfy@ugrad.math.ubc.ca
Department of Mathematics
The University of British Columbia
Room 121, 1984 Mathematics Road
Vancouver, British Columbia, Canada V6T 1Z2

ABSTRACT. This lecture notes contains all the SMS summer school material on "Counting arithmetic objects" held at the CRM in Montréal between June 23 and July 04, 2014. We would like to thank the organizers for putting together this summer school and inviting the experts to speak, and for the CRM for its hospitality.

CONTENTS

1. Introduction and Perspectives
by Manjul Bhargava

2. Algebraic groups, representation theory, and invariant theory
by Eyal Goren

3. Basic algebraic number theory (number fields, class groups)
by Eknath Ghate

4. Basics of binary quadratic forms and Gauss composition
by Andrew Granville

5. CURVES, GEOMETRIC ASPECTS
BY HENRI DARMON

6. Basic analytic number theory
by Andrew Granville

7. CURVES, DIOPHANTINES ASPECTS
BY HENRI DARMON

8. More algebraic groups, representation theory and invariant theory
by Eyal Goren

9. Cubic rings
BY MELANIE MATCHETT-WOOD

10. Quartic and quintic rings
by Melanie Matchett-Wood

11. PROBLEM SET (1/7)

11.1. **Directly from Wood's cubic rings lecture.**

(i) Prove that the inverse maps $R \to \mathrm{D}\,isc(R)$ and $D \to \mathbb{Z}[\tau]/(\tau^2 - D\tau + \frac{D^2-D}{4})$ induce a bijection between the set of quadratic rings (up to isomorphism) and

(ii) In the Delone Faddeev equations

$$\omega\theta = n, \omega^2 = m - b\omega + a\theta, \theta^2 = \ell - d\omega + c\theta,$$

prove that associativity is equivalent to the equations

$$n = -ad, \ell = -bd, m = -ac.$$

(iii) Wood mentioned that if you write $+b$ and $+d$ in place of $-b$ and $-d$ above, the correspondence comes out slightly wrong. Try it and see what happens.

(iv) Orders in cubic number fields correspond to irreducible cubic forms $f(x, y)$, and the number field can be recovered as $\mathbb{Q}[\theta]/(f(\theta, 1))$. What happens if you substitute $f(1, \theta)$ for $f(\theta, 1)$? (What *must* happen?)

(v) For a cubic form f, prove that the functions on its vanishing set V_f determine a cubic ring, which is the same ring obtained by the Delone-Faddeev correspondence. (Describe any special conditions, e.g., $f \neq 0$, which are necessary in your proof.)

11.2. **Other Exercises Concerning Cubic Rings.** We give more exercises for cubic than for quartic or quintic rings. Note that most or all of these exercises are interesting for all three parameterizations being discussed. You are *strongly encouraged* to extrapolate problems from one section to another! What is the same, and what is different?

(i) A good way to get started is to compute lots of examples of the Delone-Faddeev correspondence. (If you don't do any of the other exercises, you should probably do at least this, and the quartic and quintic analogues!) What binary cubic form f corresponds to the cubic ring $\mathbb{Z}^3$? To $\mathbb{Z}[\sqrt[3]{n}]$? Conversely, what cubic ring corresponds to the cubic form $u^3 - uv^2 + v^3$? To $u(u - v)(u + v)$? To u^3? To 0? Work out these, as well as other examples of your own invention, and compute all of their discriminants.

(ii) Another good way to get started is to work out the details of the Delone-Faddeev and Davenport-Heilbronn correspondences. The exposition given at `http://arxiv.org/pdf/1005.0672.pdf` on pp. 4-7 leaves many small details to be checked by the reader. Pick your favorite lemma or proposition and work out the proof in more detail than given in the paper.

(iii) The Delone-Faddeev correspondence is very interesting over $\mathbb{F}_p$. Assuming for simplicity that $p \neq 2, 3$, determine all of the cubic rings over $\mathbb{F}_p$ as well as the $\mathrm{GL}_2(\mathbb{F}_p)$-equivalence classes of cubic forms over $\mathbb{F}_p$. How many equivalence classes are there? On the cubic forms side, how large is each $\mathrm{GL}_2(\mathbb{F}_p)$-equivalence class, and how big is each of the corresponding stabilizer groups? If you reduce an integral binary cubic form modulo p, what is the relationship between the cubic ring over $\mathbb{Z}$ and the cubic ring over $\mathbb{F}_p$?

(iv) Work out what the Delone-Faddeev correspondence says over $\mathbb{C}$:

The fact that $\mathrm{GL}_2(\mathbb{C})$ acts prehomogeneously on binary cubic forms over $\mathbb{C}$ can be restated by saying that all nonsingular binary cubic forms form a single $\mathrm{GL}_2(\mathbb{C})$-orbit, and therefore (by Delone-Faddeev) that there is exactly one nondegenerate cubic ring over $\mathbb{C}$

up to isomorphism. Work out this case of the Delone-Faddeev correspondence, describe this cubic ring, and prove its uniqueness directly.

(v) Classify the set of those $\mathrm{GL}_2(\mathbb{Z}_p)$-orbits on $V(\mathbb{Z}_p)$ whose discriminants are not divisible by p. What about those whose discriminants are exactly divisible by p or p^2? Which of these extensions are maximal?

(vi) Let f be an element of $V(\mathbb{Z}_p)$ and let $\bar{f}$ denote its reduction modulo p. Let R_f and $R_{\bar{f}}$ denote the corresponding cubic extensions of $\mathbb{Z}_p$ and $\mathbb{F}_p$, respectively. Describe $R_{\bar{f}}$ in terms of R_f.

(vii) Let f be an integral cubic form, and let R denote the corresponding cubic ring over $\mathbb{Z}$. Show that the cubic extension of $\mathbb{Z}_p$ corresponding to the $\mathrm{GL}_2(\mathbb{Z}_p)$-orbit of f is $R \otimes \mathbb{Z}_p$.

(viii) The *content* of a ring R of a ring of rank n is the largest integer c such that $R = \mathbb{Z} + cR'$ for some ring R' of rank n. The *content* of an integral binary cubic form f is the gcd of the coefficients of f. Show that the content of an integral binary cubic form f is equal to the content of the corresponding cubic ring R.

(ix) Consider the form $\mathrm{Tr}(x^2)$ on the cubic ring $R = R(f)$. Now restrict this form to the sublattice of R consisting of elements of trace 0. What is the interpretation of this quadratic form in terms of the corresponding binary cubic f?

(x) Write down some examples of cubic rings inside Galois cubic fields. Do they all have three automorphisms? What are the associated binary cubics? What can you say about the $\mathrm{Tr}(x^2)$ form for a cubic ring having three automorphisms? Can you use this to give an explicit parametrization of such "C_3-cubic rings"?

(xi) Show that the cubic ring given by a binary cubic form lies in the field generated by the coordinates of the points cut out in $\mathbb{P}^1$ by the form. What if the field is quadratic?

(xii) What can you say about the integers represented by a binary cubic form f, making use of the relationship with the corresponding cubic ring $R(f)$?

(xiii) For all of these parameterizations, it is possible (and not terribly difficult) to write down the discriminant as an explicit $n \times n$ determinant in n variables, for $n = 4, 12, 40$ respectively.

We will outline the cubic case here (where the discriminant polynomial is otherwise easy to write down, so that it is easy to check your work!) First, use the $NAK\Lambda$ decomposition of $\mathrm{GL}_2(\mathbb{C})$ to write down a basis for the Lie algebra $\mathfrak{gl}_2(\mathbb{C})$, i.e., the tangent space of the identity of $\mathrm{GL}_2(\mathbb{C})$. For $g \in \mathfrak{gl}_2(\mathbb{C})$ and a general $v \in V_{\mathbb{C}}$, compute the infinitesimal action

$$\lim_{h \to \infty} \frac{(I + hg) \circ v - v}{h},$$

which will be a tangent vector in $V_{\mathbb{C}}$ (and a function of the four coordinates v_1, v_2, v_3, and v_4). The matrix of all of these, as g ranges over your basis for $\mathfrak{gl}_2(\mathbb{C})$, will be singular if and only if there is a local homeomorphism between a neighborhood of $I \in \mathrm{GL}_2(\mathbb{C})$ and a neighborhood of $v \in V_{\mathbb{C}}$, which will happen if and only if $\mathrm{D}\, isc(v) \neq 0$. Compute this matrix, and observe that its determinant is a degree 4 polynomial in the coordinates v_1, v_2, v_3, and v_4. Since the ring of invariants of $V_{\mathbb{C}}$ is generated by the discriminant, it follows that the determinant of your matrix is equal to $\mathrm{D}\, isc(v)$ times a scalar. By comparing with some $v \in V_{\mathbb{C}}$ for which you otherwise compute its discriminant, and probably using PARI/GP, Sage, or some other such software, determine this scalar and therefore the discriminant polynomial on $V_{\mathbb{C}}$.

11.3. **Quartic Rings.**

(i) Warm up: What pair of ternary quadratic forms corresponds to $\mathbb{Z}^4$? To $\mathbb{Z}[\sqrt[4]{n}]$? To $\mathbb{Z}[\sqrt{a}, \sqrt{b}]$? Or your favorite quartic ring?

(ii) Find pairs of ternary quadratic forms corresponding to quartic rings that have some special kind of structure – for example, those lying inside $K \oplus \mathbb{Q}$ where K is a cubic field. How does this relate to cubic rings and binary cubic forms? What about other types of special structure, such as the various possible Galois groups? Can you find nice representatives for the pairs of ternary quadratic forms corresponding to these? Can you find a parametrization space for quartic rings with one of these structures?

(iii) Show that the quartic ring given by a pair of ternary quadratic forms lies in the field generated by the coordinates of the points cut out in $\mathbb{P}^2$ by these forms. In particular, what happens in some of the special cases considered in part (b)?

(iv) What can you say about the pairs of integers represented by a pair of ternary quadratic forms in terms of the corresponding quartic ring?

(v) Oh, here's a question I like: Show that every maximal quartic ring is represented exactly once as a pair of integral ternary quadratic forms (up to equivalence).

(vi) As a generalization of the above, show that the number of cubic resolvent rings of a quartic ring Q is the number of index c sublattices of $\mathbb{Z}^2$, where c is the content of Q. [It follows, in particular, that every maximal quartic ring is represented exactly once as a pair of integral ternary quadratic forms (up to equivalence).]

(vii) For quartic (and, later, quintic) rings: similarly describe the content of a quartic ring Q in terms of the corresponding pair of integral ternary quadratic forms.

(viii) Classify the set of maximal quartic extensions of $\mathbb{Z}_p$.

(ix) Given a maximal quartic extension of $\mathbb{Z}_p$, determine its cubic resolvent ring.

11.4. **Quartic rings and their cubic resolvents.** A nondegenerate binary cubic form f over a field k determines three points in $\mathbb{P}^1_{\bar{k}}$, namely the three roots of f. This *set of three points* is defined over k, and thus consists of a union of Galois-orbits. All three points might be defined over k, or the three points could be a union of a Galois-orbits containing two points and a third point defined over k, or the three points could consist of a single Galois-orbit. (Here, $\bar{k}$ denotes the algebraic closure of k.)

Similarly, a pair (A, B) of ternary quadratic forms yields four points in $\mathbb{P}^2_{\bar{k}}$ given by the intersection of the two quadrics cut out by A and B. This *set of four points* is defined over k, and thus consists of a union of Galois-orbits. Given these four points, say P_1, P_2, P_3, P_4, we may consider the following set of pairs of lines: $\{(P_1P_2, P_3P_4), (P_1P_3, P_2P_4), (P_1P_4, P_2P_3)\}$.

Recall that given a pair (A, B) of integral ternary quadratic forms (represented a symmetric 3×3 matrices), the cubic resolvent form of (A, B) is defined to be $4\mathrm{D}\, et(Ax - By)$.

(i) Let f be a nondegenerate cubic form over $\mathbb{Q}_p$. Prove that the field of definitions of the corresponding three points determines the degree three extension of $\mathbb{Q}_p$ corresponding to f, and therefore its splitting type.

(ii) Prove the analogous problem with f replaced with a pair of ternary quadratic forms.

(iii) Given a pair of ternary quadratic forms over $\mathbb{Q}_p$, prove that the corresponding set of pairs of lines is also defined over $\mathbb{Q}_p$.

(iv) Prove that the Galois action on this set of pairs of lines is the same as the Galois action on the three points determined by the cubic resolvent.

(v) Use the above problems to determine the cubic resolvent of nondegenerate quartic extensions of $\mathbb{Q}_p$.

(vi) A nondegenerate quartic extension of $\mathbb{Q}$ could be a field (what are the possible Galois groups of the normal closure of these fields?), or a direct product of fields. In all these cases, determine the cubic resolvent of the quartic extension.

(vii) Give a convenient way of distinguishing a D_4-quartic field from an S_4-quartic field.

11.5. **Quintic Rings.**

(i) Give examples of forms corresponding to some examples of quintic rings.

(ii) Can you find a parametrization space for quintic rings with some special structure (as in 2(b))?

(iii) Let $(A, B, C, D, E) \in V(\mathbb{Q})$ correspond to the quintic extension K. Prove that if A has rank ≤ 2, then the five associated quadrics have a common zero defined over $\mathbb{Q}$ and therefore K is not a field.

(iv) Let $(A, B, C, D, E) \in V(\mathbb{Q})$ correspond to the quintic extension K, and let $Q_1, \ldots, Q_5$ be the five associated quadrics. Prove that if Q_1 factors over $\mathbb{Q}$, then K is not a field.

11.6. **Noncommutative Rings.**

(i) Consider some of the analogous questions for quaternion rings!

(ii) By taking the $\mathrm{Tr}(x^2)$ form on a quartic ring (restricted again to the trace 0 part of the ring), one obtains a ternary quadratic form, which corresponds to a quaternion ring! What is the relation between this quaternion ring and the original quartic ring?

12. How to count rings and fields (1/2)
by Manjul Bhargava

13. Rings associated to binary n-ic forms, composition of $2 \times n \times n$ boxes and class groups

by Melanie Matchett-Wood

14. THE ZETA FUNCTIONS ATTACHED TO PREHOMOGENEOUS VECTOR SPACES BY TAKASHI TANIGUCHI

15. Problem Set (2/7)

15.1. **An easy version of Davenport's lemma and some generalizations.** 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 $n-1$.

(i) **(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

$$\#\{g \cdot B \cap \mathbb{Z}^n\} = \mathrm{Vol}(g \cdot B) + O(MP(g \cdot B)), \tag{15.1}$$

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.

(ii) Modify the necessary arguments to obtain an estimate analogous to (15.1) 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

$$\#\{g \cdot B \cap \mathbb{Z}^n\} = \mathrm{Vol}(g \cdot B) \prod_{i=1}^{m} \mathrm{Vol}(L_p) + O(MP(g \cdot B)), \tag{15.2}$$

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 Z_p^n has volume 1.

(iii) Modify the necessary definitions and arguments to obtain estimates analogous to (15.1) and (15.2) when B is an open bounded multiset.

15.2. **Counting number fields using the geometry of numbers.**

(i) Granville explained how to count $\sum_{n<X} d(n)$.

Defining $d_k(n)$ to be the number of ways to write n as a product of k positive integers, prove asymptotics for $\sum_{n<X} d_k(n)$. (Bonus: prove them with lower order terms and power saving error terms.)

(ii) In Granville's solution of the circle problem, suppose that one is interested in counting only those pairs (x, y) with $x^2 + y^2 \leq X$ and $x^2 + y^2 \equiv a \pmod{q}$, for some a and q. Obtain an asymptotic formula in this case, with an error term depending explicitly on a, q, and X. Does the added condition increase or decrease the error term?

Suppose instead that you require $x \equiv a \pmod{q}$. How does this change things? (Try out some other conditions instead.)

(iii) Compute an asymptotic formula for

$$\sum_{0<-D<X} h(-D).$$

You will use Gauss's reduction theory of binary quadratic forms. Can you incorporate Bhargava's averaging method?

(iv) Without doing any involved computations, and presuming that asymptotic formulas can indeed be proved, explain why the following formulas are correct. (C stands for a different constant at each appearance.)
   (a) We have $\sum_{0<-D<X} h(-D) \sim CX^{3/2}$.
   (b) The number of cubic, quartic, and quintic rings (together with cubic or sextic resolvents in the latter two cases) R with $0 < |\mathrm{D}\, isc(R)| < X$ is $\sim CX$ in each case (with different constants).
   (c) Give a rough heuristic argument for why the proportion of such rings nonmaximal at p is roughly $\frac{1}{p^2}$, and accordingly give a rough argument for why then the number of cubic, quartic, and quintic *fields* K with $0 < |\mathrm{D}\, isc(K)| < X$ is $\sim CX$.

(v) Asymptotically there are 3 times as many cubic fields K with $|\mathrm{D}\, isc(K)| < X$ with mixed signature than which are totally real. Why 3, and not 1 or $\frac{\pi^6}{945}$? Trace the discrepancy in Bhargava, Shankar, and Tsimerman's paper, and explain where it comes from.

15.3. **Index-three subgroups in the class groups of quadratic fields.** Let K_2 be a fixed quadratic field. Recall that Class Field Theory implies that the maximal unramified extension of K_2 is Galois over K_2 with Galois group isomorphic to the class group of K_2. Thus, index-3 subgroups of the class group of K_2 are in bijection with degree 3-unramified extensions of K_2.

(i) Let K_{2p} be a degree-p unramified extension of K_2. By studying the action of σ, the non trivial automorphism of K_2, prove that K_{2p} is Galois over $\mathbb{Q}$.
(ii) Prove that the Galois group of K_{2p} is not cyclic.
(iii) We now restrict to the case when $p = 3$. We know that K_6 is a Galois S_3 field. Let K_3 denote one of its cubic subfields. By reading this wonderful one page write up of Wood's: `http://www.math.wisc.edu/~mmwood/Splitting.pdf`, determine how primes split in K_3 in terms of how they split in K_2.
(iv) From the above problem, classify the possible cubic fields that can arise as K_3's. We call these *nowhere totally ramified* cubic fields.
(v) Let K_3 be a nowhere totally ramified cubic S_3 field, let K_6 be its Galois closure, and let K_2 be the quadratic subfield of K_6. Prove that K_6 is unramified over K_2.
(vi) Prove that the discriminant of K_3 is the same as the discriminant of K_2.
(vii) Use the above problems, and the results counting cubic fields to compute the average size of the 3-torsion in the class groups of quadratic fields.

15.4. **Binary n-ic forms and the ring associated to them.**

(i) Repeat Problem 1e of the previous problem set for rings associated to binary n-ic forms.
(ii) Given a integral binary n-ic form f, construct an integral $2 \times n \times n$ box whose resolvent is f.
(iii) Let n be odd. Given a integral binary n-ic form f, construct a $\mathbb{Z}^2 \times \mathrm{Sym}^2(\mathbb{Z}^n)$ box whose resolvent is f.
(iv) Why does the above solution fail when n is even? Can you construct a binary quartic form f such that no $\mathbb{Z}^2 \times \mathrm{Sym}^2(\mathbb{Z}^4)$ box has f as a resolvent?

15.5. **Poisson Summation.** Another tool that can be used to count lattice points is Poisson Summation. Let $f : \mathbb{R}^n \to \mathbb{C}$ be an L^2 function. Let $\hat{f} : \mathbb{R}^n \to \mathbb{C}$ denote the Fourier transform of f.

Then we have the Poisson summation formula:

$$\sum_{v\in\mathbb{Z}^n} f(v) = \sum_{v\in\mathbb{Z}^n} \hat{f}(v). \tag{15.3}$$

(i) **Counting smoothly** Let χ_B denote the characteristic function of $B \subset \mathbb{R}^n$. We can write

$$\#\{g\cdot B \cap \mathbb{Z}^n\} = \sum_{v\in\mathbb{Z}^n} g\cdot\chi_B(v), \tag{15.4}$$

where $\mathrm{GL}_n(\mathbb{R})$ acts on the space of functions $f : \mathbb{R}^n \to \mathbb{C}$ via $g\cdot f(v) := f(g^{-1}v)$. (Check that this is a right action of $\mathrm{GL}_n(\mathbb{R})$ and that under this action $g\cdot\chi_B = \chi_{g\cdot B}$.)

To count "smoothly", we replace the characteristic function of B in (15.4) by a smooth function f with compact support.

(ii) Prove smooth versions of the easy version of Davenport's Lemma and its generalizations by using the Poisson summation formula. Note that in many cases the error term is substantially improved. For which $g \in \mathrm{GL}_n(\mathbb{R})$ does the error term stay the same?

15.6. **Zeta functions associated to prehomogeneous vector spaces.**

(i) (*The Riemann zeta function*) The Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

is the simplest example of a zeta function associated to a prehomogeneous vector space. We will review the proof of its functional equation.

(a) Prove that

$$Z(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s) = \frac{1}{2}\int_0^\infty \Big(\sum_{n\in\mathbb{Z}-\{0\}} e^{-\pi n^2 y}\Big) y^{s/2}\frac{dy}{y}.$$

State explicitly any conditions on s which you assume in the course of your proof. (Recall the definition of the *gamma function*: it is the Mellin transform of the function e^{-t}, namely

$$\Gamma(s) = \int_0^\infty e^{-t}t^s\frac{dt}{t}.$$

(b) Use the *Poisson summation formula* to prove that

$$\sum_{n\in\mathbb{Z}} e^{-\pi n^2 y} = y^{1/2}\cdot\sum_{n\in\mathbb{Z}} e^{-\pi n^2/y}.$$

This *modularity relation* illustrates the importance of the function $e^{-\pi n^2 y}$, and indirectly explains why the gamma function is needed to 'complete' the Riemann zeta function. (For the best explanation of this phenomenon, read *Tate's thesis*.

(c) By splitting the integral into intervals $(0,1)$ and $(1,\infty)$, and using the Poisson sum formula on the former, prove that

$$Z(s) = \frac{1}{2}\int_0^\infty \Big(\sum_{n\in\mathbb{Z}-\{0\}} e^{-\pi n^2 y}\Big) y^{s/2}\frac{dy}{y} - \int_0^1 y^{s/2}\frac{dy}{y} + \frac{1}{2}\sqrt{y}\int_0^\infty \Big(\sum_{n\in\mathbb{Z}} e^{-\pi n^2 y}\Big) y^{1/2-s/2}\frac{dy}{y}.$$

(d) Explain why the zeta function would have been much nicer (and, in particular, entire) if it only included the term $\frac{1}{0^s}$. (The question is quite vague, but pondering it illustrates some of the technical difficulties inherent in Shintani's work.)

(ii) Let $f : V_{\mathbb{R}} \to R$ be a nice test function defined on the space of binary cubic forms, and recall that the completed Shintani zeta function is defined by the formula

$$Z(f,s) := \int_{\mathrm{GL}_2^+(\mathbb{R})/\mathrm{SL}_2(\mathbb{Z})} (\det(g))^{2s} \sum_{x \in V_{\mathbb{Z}} - S} f(gx) dg,$$

where S is the set of points $x \in V_{\mathbb{Z}}$ with $|\mathrm{D}\, isc(x)| = 0$.

(a) Verify that $\mathrm{D}\, isc(gx) = (\det(g))^2 \mathrm{D}\, isc(x)$.

(b) Suppose that f is supported in $V_{\mathbb{R}}^+$, i.e., on binary cubic forms with positive discriminant. Carrying out a Jacobian change of variables formula, prove (Shintani, p. 153, Prop. 2.4) that

$$\int_{\mathrm{GL}_2^+(\mathbb{R})} f(gy) dg = \frac{1}{4\pi} \int_{V^+(\mathbb{R})} |\mathrm{D}\, isc(x)|^{-1} f(x) dx.$$

If f is instead supported in $V^-(\mathbb{R})$, prove the analogous formula , only with $\frac{1}{4\pi}$ replaced with $\frac{1}{12\pi}$.

(c) Using the above, prove the formula

$$Z(f,s) = \frac{1}{4\pi}\xi^+(s) \int_{V^+} |\mathrm{D}\, isc(x)|^{s-1} f(x) dx + \frac{1}{12\pi}\xi^+(s) \int_{V^+} |\mathrm{D}\, isc(x)|^{s-1} f(x) dx.$$

(d) Redo all of the above, only for the simplest prehomogeneous vector space: replace $V_{\mathbb{R}}$ with $\mathbb{R}$, $V_{\mathbb{Z}}$ with $\mathbb{Z}$, and $\mathrm{D}\, isc(x)$ with x. What formula do you obtain? If you choose the test function $f(x) = e^{-x^2}$, you should recognize something especially familiar. What?

15.7. **Counting squarefree integers less than X.** *This exercise will be highly relevant to the Friday and Saturday lectures. You might wait until after these lectures to do these problems, or attempt this to get a preview.*

Let $[X]$ denote the set of positive integers $n \leq X$, and let $[X]^{\mathrm{sf}}$ denote the subset of integers $n \in [X]$ that are squarefree. Our aim is to prove that $\lim_{X\to\infty} \frac{\#[X]^{\mathrm{sf}}}{\#[X]} = \frac{1}{\zeta(2)}$.

(i) Let Y be a fixed positive integer, and let $[X]^{\mathrm{sf},Y}$ denote the set of elements in $[X]$ that are not divisible by p^2 for primes $p \leq Y$. Prove that

$$\lim_{X\to\infty} \frac{\#[X]^{\mathrm{sf},Y}}{\#[X]} = \prod_{p \leq Y} (1 - 1/p^2).$$

(ii) By taking limit $Y \to \infty$ conclude that $\lim_{X\to\infty} \frac{\#[X]^{\mathrm{sf}}}{\#[X]} \leq \frac{1}{\zeta(2)}$.

(iii) (**Tail estimate**) Prove that the number of positive integers less than X that are divisible by p^2 is bounded by $O(X/p^2)$, where the implied constant is independent of X and p.

(iv) Use the tail estimate to prove that

$$\#[X]^{\mathrm{sf}} = \#[X]^{\mathrm{sf},Y} + O(\sum_{p>Y} X/p^2).$$

Divide by X and take limits (first $X \to \infty$ then $Y \to \infty$) to conclude the desired result.

Note that the above list of problems proves that $\#[X]^{\mathrm{sf}} = \frac{\#[X]}{\zeta(2)} + o(X)$. We can use the inclusion-exclusion formula to improve the error term $o(X)$ to a power saving of X. To this end, let $[X]_{a\,(b)}$ denote the subset of integers $n \in [X]$ such that $n \equiv a \pmod{b}$.

(i) Prove the inclusion-exclusion formula

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

and use it to prove that $\#[X]^{\mathrm{sf}} = \frac{\#[X]}{\zeta(2)} + O(X^{1/2})$.

(ii) Replace the "sharp" count $\#[X]$ and $\#[X]^{\mathrm{sf}}$ by "smooth" counts. (Replace the characteristic function of the unit interval $[0,1]$ with a smooth approximation of it.) Estimate the smooth analogue of $\#[X]^{\mathrm{sf}}$ using inclusion exclusion. Note that the gains of counting smoothly are lost in the sieve.

(iii) Count cubefree integers both sharply and smoothly.

16. How to count rings and fields (2/2)
by Manjul Bhargava

17. Heuristics for number field counts and applications to curves over finite fields

by Melanie Matchett-Wood

18. Moduli space of rings
by Bjorn Poonen

19. Problem Set (3/7)

20. Zeta Function methods
BY Frank Throne

21. Counting Artin representations and modular forms of eight one by Eknath Ghate

22. Binary quartic forms; bounded average rank of elliptic curves by Arul Shankar (1/2)

23. Selmer groups and heuristics (1/2)
by Bjorn Poonen

24. Rational points on curves
by Michael Stoll

25. Problem Set (4/7)

26. BINARY QUARTIC FORMS; BOUNDED AVERAGE RANK OF ELLIPTIC CURVES BY ARUL SHANKAR (2/2)

27. Coregular spaces and genus one curves
by Wei Ho

28. Arithmetic invariant theory and hyperelliptic curves (1/2)

by Benedict Gross

29. Problem Set (5/7)

30. Applications to the Birch and Swinnerton-Dyer conjecture by Manjul Bhargava

31. Selmer groups and heuristics (2/2)
by Bjorn Poonen

32. Arithmetic invariant theory and hyperelliptic curves (2/2)

by Benedict Gross

33. Problem Set (6/7)

34. Chabauty methods and hyperelliptic curves
by Bjorn Poonen

35. Topological and algebraic geometry method over function fields (1/2)
by Jordan Ellenberg

36. Counting methods over global fields
BY JERRY WANG

37. Problem Set (7/7)

38. The Chabauty method and symmetric powers of curves
by Jennifer Park

39. Topological and algebraic geometry methods over function fields (2/2)
by Jordan Ellenberg

40. Future perspectives
by Manjul Bhargava