Sieve methods in arithmetic statistics

Andrew O'Desky

Last updated May 19, 2024

These are lecture notes on sieve methods in arithmetic statistics which were used for a graduate seminar at Princeton University in Spring 2024. Two problems from arithmetic statistics are studied: the density of squarefree values of polynomials, and the number of cubic abelian trace-one polynomials with bounded integer coefficients.

Table of Contents

1 Squarefree values of polynomials

1.1 Motivation

Let $f(x_1, \ldots, x_m)$ be a polynomial with integer coefficients and for $a \in \mathbb{Z}^m$ let $|a| = \max(|a_1|, \ldots, |a_m|)$. Assume that f is squarefree.

The (natural) density of squarefree values of f is the limit

$$\lim_{X \to \infty} \mathbb{P}(f(a) \text{ is squarefree} : a \in \mathbb{Z}^m, |a| < X) = \lim_{X \to \infty} \frac{\#\{a \in \mathbb{Z}^m : |a| < X, f(a) \text{ squarefree}\}}{(2X+1)^m}.$$

Conjecturally, this density exists and is positive.

Squarefree values of polynomials are important in arithmetic statistics. We are often interested in prehomogeneous spaces: a linear representation V of an algebraic group with a dense open orbit whose points parametrize some objects of arithmetic interest (usually orders or curves with some structure), and there is a natural discriminant-like polynomial $f \colon V \to \mathbb{A}^1$ such that $\{f \neq 0\}$ is the open orbit.

Intuitively, the values of f measure how closely a point approaches the discriminant locus $\{f = 0\} \subset V$, and squarefree values of f are attained at points which do not get too close to the discriminant locus (in the sense of heights).

For instance, the space $V = \mathrm{Sym}^3(\mathbb{A}^2)$ of binary cubic forms parametrizes cubic orders with a $\mathbb{Z}$-basis of the form $(1, \alpha, \beta)$ satisfying $\alpha\beta \in \mathbb{Z}$. The discriminant polynomial is given by

$$f(ax^3 + bx^2y + cxy^2 + dy^3) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

In the context of van der Waerden's conjecture, we are interested in the affine space V of all monic polynomials of degree n, and the discriminant polynomial

$$f(x^n + a_1x^{n-1} + \cdots + a_n) = \mathrm{disc}(x^n + a_1x^{n-1} + \cdots + a_n).$$

Recall that polynomials with small Galois group have large index, and the discriminant will be divisible by large powers.

Those polynomials with squarefree discriminant will have Galois group S_n, and other nice properties such as having a monogenic ring of integers.

Squarefree discriminants correspond to the simplest type of ramification, namely two points coming together. In moduli problems allowing for different types of ramification this typically corresponds to the generic situation.

Remark 1.1. For a geometric analogue, consider Hurwitz spaces $\mathcal{H}_R$ which parametrize the set of covers of the projective line with a given ramification type R. In the analogy between algebraic curves and number fields, the genus is analogous to $\log(\sqrt{\text{disc}})$. By the Riemann–Hurwitz formula,[1] each critical value Q contributes

$$\sum_{P/Q} \tfrac{1}{2}(e_P - 1)$$

to the genus of the curve. This shows that covers with ramification worse than simple are sparse when measured by discriminant.

What is known?

First note that the density of p-squarefree values for a *fixed* prime p is easy to compute. This is because whether or not p^2 divides $f(a)$ is determined by the residue $a \pmod{p^2} \in (\mathbb{Z}/p^2\mathbb{Z})^m$. So

$$\mathbb{P}(f(a) \text{ is } p\text{-squarefree}) = \lim_{X\to\infty} \mathbb{P}(f(a) \text{ is } p\text{-squarefree} : a \in \mathbb{Z}^m, |a| < X) = 1 - c_p/p^{2m}$$

where $c_p = \#\{a \in (\mathbb{Z}/p^2\mathbb{Z})^m : f(a) \equiv 0 \pmod{p^2}\}$. This extends to squarefree conditions at *finitely* many primes by the Chinese Remainder Theorem.

Conjecturally, for almost all a we expect the divisibilities of $f(a)$ at different primes to be independent quantities. This would imply that the density of squarefree values for a squarefree polynomial $f \in \mathbb{Z}[x_1, \dots, x_m]$ is equal to

$$\prod_p \mathbb{P}(f(a) \pmod{p^2} \text{ is squarefree}) = \prod_p (1 - c_p/p^{2m}).$$

Assuming the *abc* conjecture, Granville [Gra98] showed this formula holds for one variable polynomials. Poonen has shown the formula for multivariable polynomials from the *abc* conjecture, however with a weaker notion of density.

Remark 1.2. *Does the multivariate case reduce to the one variable case?* Consider the two

[1] for a nonconstant separable morphism $f\colon X \to Y$ of smooth projective curves, we have $2g_X - 2 = (2g_Y - 2)\deg f + \sum_P (e_P - 1)$.

variable case $f(x,y)$, supposing we know the one variable case to be true. Write $f_a(y) = f(a,y)$. Then

$$\sum_{-X/2\le a,b\le X/2} 1_{\mathrm{sqf}}(f(a,b)) = \sum_{-X/2\le a\le X/2} (X\delta_{f_a} + o(X)) \overset{?}{=} X^2\delta_f + o(X^2).$$

So we may relate the problem of squarefree densities for $f(x,y)$ to an averaged problem for the *family* of polynomials $\{f_a : a \in \mathbb{Z}\}$. The question is whether the one-variable densities average to the two-variable density:

$$\frac{1}{X}\sum_{-X/2\le a\le X/2} \delta_{f_a} \overset{?}{=} \delta_f + o(1).$$

This is true (for trivial reasons) for the *local* densities, but for the global densities it is unclear why the average of the product of local densities should be equal to the product over the averages of the local densities.

Conjecture 1.3 (*abc* conjecture. Oesterlé, Masser, Szpiro)**.** *Fix $\varepsilon > 0$. If a,b,c are coprime positive integers satisfying $a+b=c$, then*

$$c \ll_\varepsilon N(a,b,c)^{1+\varepsilon}$$

where $N(a,b,c)$ is the product of the distinct primes dividing abc.

For one variable polynomials, degrees 1 and 2 are relatively easy. Degree 3 was proven by Hooley [Hoo68]. Degrees ≥ 4 are open.

For binary homogeneous forms, it is known up to degree 6 by Greaves [Gre92]. Degrees ≥ 7 are open.

For the discriminant of monic, resp. general polynomials of a fixed degree, it was proven by Bhargava–Shankar–Wang [BSW22a], resp. [BSW22b].

But in most cases it is even unknown whether a given squarefree polynomial takes infinitely many squarefree values, e.g. x^4+2.

The density of squarefree numbers

Reference: [Bha21, 13]. An instructive case is estimating the number of squarefree numbers between 1 and X, corresponding to $f(x) = x$.

Theorem 1.4. *The natural density of integers that are squarefree is* $1/\zeta(2) = 6/\pi^2 = .6079\ldots$.

In this one variable setting our heuristic is that for integers, the property of being squarefree satisfies a "local-to-global principle", so the probability of being squarefree is

$$\prod_p (1 - 1/p^2) = 1/\zeta(2).$$

Proof. Let $S_p = \{m : p^2 \nmid m\}$. By the Chinese Remainder Theorem, for any $Y > 0$ we have that

$$\lim_{X\to\infty} \frac{\#\{m \in \cap_{p<Y} S_p : |m| < X\}}{\#\{m : |m| < X\}} = \prod_{p<Y} (1 - 1/p^2).$$

That is to say, the Chinese Remainder Theorem assures independence for a *finite* set of primes $\{p : p < Y\}$. Since

$$\cap_{p<Y} S_p \supset \cap_p S_p = \{m : m \text{ squarefree}\},$$

we trivially get the upper bound

$$\limsup_{X\to\infty} \frac{\#\{m \text{ squarefree} : |m| < X\}}{\#\{m : |m| < X\}} \leq \prod_{p<Y} (1 - 1/p^2)$$

so taking Y to infinity shows that $\zeta(2)^{-1}$ is the correct upper bound.

For the lower bound, observe that

$$\bigcap_{p<Y} S_p \subset \{m : m \text{ squarefree}\} \cup \bigcup_{p\geq Y} S_p^c$$

since any integer in the left-hand set is either squarefree or divisible by p^2 for some $p \geq Y$.

The number of $m \in \mathbb{Z}$ divisible by p^2 with $|m| < X$ is $2X/p^2 + O(1)$. So

$$\begin{aligned} \frac{\#\{m \in \cap_{p<Y} S_p : |m| < X\}}{\#\{m : |m| < X\}} &\leq \frac{\#\{m \text{ squarefree} : |m| < X\}}{\#\{m : |m| < X\}} + \sum_{\sqrt{X}>p\geq Y} \frac{2X/p^2 + O(1)}{\#\{m : |m| < X\}} \\ &\leq \frac{\#\{m \text{ squarefree} : |m| < X\}}{\#\{m : |m| < X\}} + \sum_{\sqrt{X}>p\geq Y} (1/p^2 + O(1/X)). \end{aligned}$$

Taking the $\liminf$ as $X \to \infty$ shows that

$$\prod_{p<Y}(1-1/p^2) \leq \liminf_{X\to\infty} \frac{\#\{m \text{ squarefree} : |m| < X\}}{\#\{m : |m| < X\}} + \sum_{p\geq Y} 1/p^2.$$

(Note the second term on the right is *finite*.) Thus taking $Y \to \infty$ shows the correct lower bound. □

In fact, we can get a power-saving error term: the number of integers n with $|n| < X$ that are squarefree is

$$X/\zeta(2) + O(\sqrt{X}).$$

Let q denote a squarefree integer and let $W_q = \cap_{p|q} S_p^c$ denote the set of positive integers divisible by q^2. Write $W(X)$ for $\#\{x \in W : |x| < X\}$. By the inclusion-exclusion principle, we have that

$$\begin{aligned}\#\{m \in S : |m| < X\} &= W_1(X) - \sum_p W_p(X) + \sum_{p,p'} W_{pp'}(X) - \sum_{p,p',p''} W_{pp'p''}(X) + \cdots \\ &= \sum_{1\leq q\leq\sqrt{X}} \mu(q) W_q(X)\end{aligned}$$

where $p, p', p'', \ldots$ denote distinct primes. (This is sometimes called the "inclusion-exclusion sieve".) This expresses S in terms of the simpler sets W_q with density $1/q^2$. Then

$$\begin{aligned}\sum_{1\leq q\leq\sqrt{X}} \mu(q) W_q(X) &= \sum_{1\leq q\leq\sqrt{X}} \mu(q)(X/q^2 + O(1)) \\ &= \left(\sum_{1\leq q\leq\sqrt{X}} \mu(q)/q^2\right) X + O(\sqrt{X}) \\ &= \left(\sum_{q=1}^{\infty} \mu(q)/q^2\right) X + O\left(\sqrt{X} + \sum_{q=\sqrt{X}}^{\infty} X/q^2\right) \\ &= \zeta(2)^{-1} X + O(\sqrt{X}).\end{aligned}$$

Note that the trivial bound $\sum_{q=1}^{Y} \mu(Y) = O(Y)$ can be improved to $\sum_{q=1}^{Y} \mu(Y) = o(Y)$, and even $O(Y^{1/2+\varepsilon})$ under the Riemann hypothesis.

The exact same argument proves that

$$\#\{m \text{ is } k\text{-powerfree} : |m| < X\} = \zeta(k)^{-1} X + O(X^{1/k}).$$

Conjecturally, the error term is $O(X^{1/(2k)+\varepsilon})$.

The best known error term, assuming the Riemann hypothesis, is $O(X^{11/35+\varepsilon})$ due to [Liu16].

1.1.1 Zeta function methods

When we have a good handle on the Dirichlet series associated to the set whose density we want to bound, it is possible to use Tauberian methods.

For k-powerfree integers ($k \geq 2$), observe that

$$\sum_{n\geq 1,\ k\text{-p.f.}} n^{-s} = \prod_p \left(1 + p^{-s} + \cdots + p^{-(k-1)s}\right) = \prod_p \frac{1-p^{-ks}}{1-p^{-s}} = \frac{\zeta(s)}{\zeta(ks)}.$$

When the generating Dirichlet series of a set has meromorphic continuation beyond the region of absolute convergence and does not grow too fast in vertical strips in the region of meromorphic continuation, Tauberian theorems express terms in the asymptotic expansions for $\#\{m \text{ is } k\text{-powerfree} : |m| < X\}$ in terms of polar data of the Dirichlet series.

From this explicit formula, we see that the poles with positive real part are at $s = 1$ with residue $1/\zeta(k)$ (the leading term in the asymptotic expansion) and $s = \rho/k$ where ρ is any nontrivial zero of $\zeta(s)$.

1.2 Strong/weak multiples

Our approach will be to separate the inputs a where p^2 divides $f(a)$ into two kinds of points, and then to handle these with different methods.

Let $f \in \mathbb{Z}[x_1, \ldots, x_m]$ and $a \in \mathbb{Z}^m$. Suppose the value $f(a)$ is exactly divisible by p^k for some $k \geq 2$. We associate to a the smallest integer j satisfying

$$a' \equiv a \pmod{p^j} \implies f(a') \equiv f(a) \pmod{p^k},$$

and say that p^k divides $f(a)$ for mod p^j reasons.

Definition 1.5. If p^k divides $f(a)$ for mod p reasons, then we say that $f(a)$ is strongly a multiple of p^k, otherwise if $j \geq 2$ we say $f(a)$ is weakly a multiple of p^k.

Geometrically speaking, when $f(a)$ is exactly divisible by p^k for $k \geq 2$ it means that the section determined by a intersects with the hypersurface $\{f = 0\}$ over p, and even remains close to X in a neighborhood.

A large j ($j \approx k$) means that $\{f = 0\}$ has large curvature near the intersection point, whereas a low value of j ($j \approx 1$) means $\{f = 0\}$ has less than expected curvature. Therefore we expect that f changes slowly p-adically near strong multiples.

In the van der Waerden proof the following proposition came up for the special case $k = 2$.

Proposition 1.6. *Assume $p > k$. If f is strongly a multiple of p^k at $a = (a_1, \dots, a_n) \in \mathbb{Z}^n$, then*

$$f(a) \equiv \frac{\partial f}{\partial x_n}(a) \equiv \cdots \equiv \frac{\partial^{k-1} f}{\partial x_n^{k-1}}(a) \equiv 0 \pmod{p}.$$

Remark 1.7. If not all the coefficients of f vanish at a as a polynomial in x_n modulo p, then the conclusion of the proposition is equivalent to the polynomial $f(a_1, \dots, a_{n-1}, x_n) \pmod{p}$ having a root of multiplicity k at $x_n \equiv a_n \pmod{p}$. (This equivalence requires $p > k$, e.g. for $k = p$ every derivative of $f = x^k$ is zero mod p.)

Proof. We will prove something stronger: for each integer $1 \leq j < k$,

$$\frac{\partial^j f}{\partial x_n^j}(a) \equiv 0 \pmod{p^{k-j}}.$$

We may by translating suppose that $a = 0$, and without loss of generality take $n = 1$. We have the finite Taylor expansion:

$$f(x) = f(0) + f'(0)x + \cdots .$$

Let $z = px$, in which case each coefficient with respect to z is a p-adic integer and we may reduce the Taylor expansion mod p^k. By assumption,

$$f(0) + f'(0)pz + \cdots \equiv f'(0)pz + \cdots \equiv 0 \pmod{p^k}.$$

If $k = 1$ we are done, and otherwise this shows that

$$f'(0)pz \equiv 0 \pmod{p^2}$$

for all $z \in \mathbb{Z}/p^k\mathbb{Z}$ and thus p divides $f'(0)$. If $k = 2$ we are done, and otherwise

$$f'(0)pz + \tfrac{1}{2!}f''(0)p^2z^2 \equiv \left(\frac{f'(0)}{p} + \tfrac{1}{2!}f''(0)z\right)p^2z \equiv 0 \pmod{p^3}$$

for all $z \in \mathbb{Z}/p^k\mathbb{Z}$. This shows that the polynomial

$$\left(\frac{f'(0)}{p} + \tfrac{1}{2!}f''(0)z\right) z \pmod p$$

evaluates to zero on any $z \in \mathbb{Z}/p\mathbb{Z}$. Since $p > k \geq 3 > 2$, this shows that each coefficient must be divisible by p. In particular, p^2 divides $f'(0)$ and p divides $f''(0)$. If $k \geq 4$ then the same argument shows that p^3 divides $f'(0)$, p^2 divides $f''(0)$, and p divides $f'''(0)$, and so on. □

Corollary 1.8. *Let f be an irreducible integral polynomial in $n \geq 2$ variables. Then there is a subvariety Y of $\mathbb{A}^n_{\mathbb{Q}}$ of codimension two such that for all but finitely many primes p,*

$$\{a \in \mathbb{Z}^n \mid f \textit{ is strongly a multiple of } p^2 \textit{ at } a\} \subseteq \{a \in \mathbb{Z}^n \mid a \pmod p \in Y(\mathbb{F}_p)\}.$$

Proof. If f is linear, then f cannot be a strong multiple of p^2 at a, so the left-hand set is empty and the assertion is vacuously true.

If f is nonlinear, there is some coordinate, say x_n, such that $\partial_n f$ is a nonconstant polynomial. Let $Y = \{f = \partial_n f = 0\} \subset \mathbb{A}^n_{\mathbb{Q}}$. The proposition shows that the left-hand set is contained in the right-hand set. The restriction of $\partial_n f$ to the irreducible hypersurface $\{f = 0\}$ cannot be constant (otherwise f would divide $\partial_n f - c$ for some constant c which would imply $\partial_n f = c$ everywhere). Therefore Y is codimension two in $\mathbb{A}^n_{\mathbb{Q}}$. □

The property of a lattice point of reducing mod p to a point on a subvariety of large codimension is precisely what the geometric sieve constrains. Thus the number of strong multiples of p^2 can be bounded by the geometric sieve, however the weak multiples typically require ad hoc arguments.

Example 1.9. Let $f = x_1x_3 + x_2x_3^2$ and $a = (p, p, p)$. Then for any integers u, v, w divisible by p, $f(p+u, p+v, p+w)$ is $O(p^2)$, so f is a multiple of p^2 at a for mod p^2 reasons.

$$\begin{aligned}
f(x_1, p, p) &= px_1 + p^3, \quad \partial_1 f(x_1, p, p) = p,\\
f(p, x_2, p) &= p^2 + p^2x_2, \quad \partial_2 f(p, x_2, p) = p^2,\\
f(p, p, x_3) &= x_3p + x_3^2p, \quad \partial_3 f(p, p, x_3) = p + 2x_3p.
\end{aligned}$$

We see that all the partials are divisible by p.

Exercises: Let $f \in \mathbb{Z}[x]$ be monic. Prove the following:

1. Prove or disprove: if $f(k)$ is divisible by a square for all $k \in \mathbb{Z}$, then $f(x) \in \mathbb{Z}[x]$ is divisible by the square of an irreducible polynomial in $\mathbb{Z}[x]$.

2. The discriminant of f is a multiple of p^2 for mod p reasons if and only if $f \pmod{p}$ has a root of multiplicity at least 3 or two roots of multiplicity at least 2.

3. The discriminant of f is a multiple of p^2 for mod p^2 reasons if and only if there exists $k \in \mathbb{Z}$ such that $f(x+k)$ has constant coefficient divisible by p^2 and linear coefficient divisible by p.

4. Use the same technique as we did for $f(x) = x$ to determine the density of squarefree values of a monic squarefree quadratic polynomial $f(x) \in \mathbb{Z}[x]$.

1.3 The geometric sieve

What is a sieve? Generally speaking, a sieve is an upper bound for the number of rational points of bounded height which satisfy specified local conditions. Typically this means that we want to find good upper bounds for the size of sets of the form

$$\{a \in \mathbb{Z}^n : |a| < X,\ a \pmod{q} \in C_q \text{ for all prime powers } q\}$$

where $C_q \subset (\mathbb{Z}/q\mathbb{Z})^n$ is some subset of local conditions at the prime power q. There are many different kinds of sieves depending on what sort of information we have about the C_q's.

The following sieve is due to Manjul Bhargava [Bha14], building on work of Ekedahl [Eke91]. We will call it the "geometric sieve".

Theorem 1.10 ([Bha14], slide 159)**.** *Fix an integer $2 \leq k \leq n$. Let B be a compact region in $\mathbb{R}^n$ having finite measure, and let Y be any closed subvariety of $\mathbb{A}^n_{\mathbb{Q}}$ whose irreducible components have codimension at least k. Let r and M be positive real numbers. Then as r and M go to infinity, possibly independently, we have that*

$$\#\{a \in rB \cap \mathbb{Z}^n \mid a \pmod{p} \in Y(\mathbb{F}_p) \text{ for some prime } p > M\}$$
$$= O\left(\frac{r^n}{M^{k-1}\log M} + r^{n-k+1}\right)$$

where the implied constant depends only on B and on Y.

The proof uses elimination theory: algebraic techniques from the 19th century for eliminating variables from generating sets of ideals in polynomial rings.

1.3.1 Resultants

The resultant is a computational tool for finding equations of projections of intersections of hypersurfaces.

Let $f = a_0x^d + a_1x^{d-1} + \cdots + a_d$ and $g = b_0x^e + b_1x^{e-1} + \cdots + b_e$ be nonzero polynomials of degrees d and e, respectively, with coefficients in a unique factorization domain A. Assume f and g are not both constant. Let $\mathcal{P}_i$ denote the free A-module of rank i generated by polynomials over A of degree $< i$.

The resultant $\operatorname{Res}(f, g)$ of f and g is defined to be the determinant of the map

$$\begin{aligned} \mathcal{P}_e \times \mathcal{P}_d &\to \mathcal{P}_{d+e} \\ (P, Q) &\mapsto fP + gQ. \end{aligned}$$

It is equal to the $(d + e) \times (d + e)$ determinant

$$\operatorname{Res}(f, g) = \det \begin{pmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \cdots & 0 & b_1 & b_0 & \cdots & 0 \\ a_2 & a_1 & \ddots & 0 & b_2 & b_1 & \ddots & 0 \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 \\ a_d & a_{d-1} & \cdots & \vdots & b_e & b_{e-1} & \cdots & \vdots \\ 0 & a_d & \ddots & \vdots & 0 & b_e & \ddots & \vdots \\ \vdots & \vdots & \ddots & a_{d-1} & \vdots & \vdots & \ddots & b_{e-1} \\ 0 & 0 & \cdots & a_d & 0 & 0 & \cdots & b_e \end{pmatrix}$$

where there are e columns with a's and d columns with b's. In the degenerate case when f and g are both nonzero constants, we set $\operatorname{Res}(f, g) = 1$. The resultant is thus an integer polynomial in the coefficients of f and g, defined whenever $f, g \neq 0$.

The key properties of the resultant: (assume f and g not both constant)

1. $\operatorname{Res}(f, g) = 0$ if and only if f and g have a nonconstant common factor in $A[x]$.

2. $\operatorname{Res}(f, g) = fP + gQ$ for some polynomials $P \in \mathcal{P}_e$ and $Q \in \mathcal{P}_d$ (these are uniquely

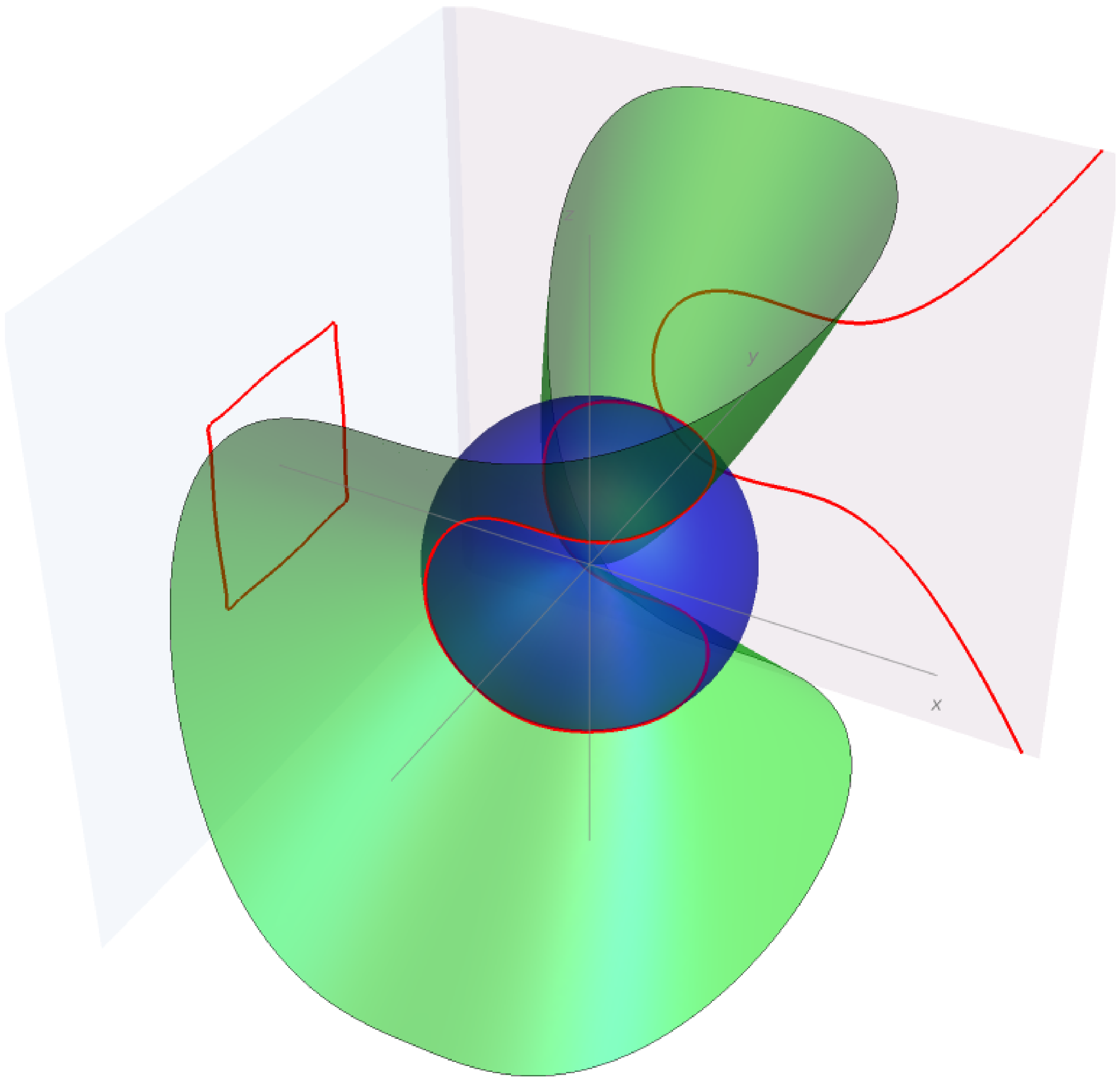

Figure 1: The intersection $V(x^2+y^2+z^2-2)\cap V(x^3+y^2-z^2)$ and two of the three resultants.

determined if f and g are coprime).

Note that (2) is a strong form of the gcd property of PIDs: when $\mathrm{Res}(f,g) \neq 0$ we can write $1 = fP_0 + gQ_0$ for $P_0, Q_0 \in \mathrm{Frac}(A)[x]$, which however only shows that

$$\mathrm{Res}(f,g) = fP + gQ$$

for polynomials $P, Q \in \mathrm{Frac}(A)[x]$.

The resultant can be used to eliminate variables from generating sets of ideals, at the cost of potentially enlarging the variety.

Lemma 1.11. *Let $f_1, \dots, f_k \in k[x_1, \dots, x_n] = A[x_n]$ be nonconstant polynomials where $A = k[x_1, \dots, x_{n-1}]$ and k is a field. Then*

$$V(f_1, \dots, f_k) \subset V(\mathrm{Res}_{x_n}(f_1, f_k), \dots, \mathrm{Res}_{x_n}(f_{k-1}, f_k), f_k).$$

Proof. By the second property of the resultant, there are polynomials P_j and Q_j for each $1 \leq j < k$ such that $\mathrm{Res}_{x_n}(f_j, f_k) = f_jP_j + f_kQ_j$. This shows that

$$(\mathrm{Res}_{x_n}(f_1, f_k), \dots, \mathrm{Res}_{x_n}(f_{k-1}, f_k), f_k) \subset (f_1, \dots, f_k)$$

which proves the containment of the associated affine varieties. □

The idea is that these $k-1$ resultants are regular functions on $\mathbb{A}^{n-1}$ which vanish on the image of $V(f_1, \dots, f_k)$ under the projection map $\mathbb{A}^n \to \mathbb{A}^{n-1}\colon (a_1, \dots, a_n) \mapsto (a_1, \dots, a_{n-1})$.

Example 1.12. Let $f = xy - 1$ and $g = x^2 + y^2 - 4$. Then

$$\mathrm{Res}_x(f,g) = \det \begin{pmatrix} y & 0 & 1 \\ -1 & y & 0 \\ 0 & -1 & y^2 - 4 \end{pmatrix} = y^4 - 4y^2 - 1.$$

By solving for the roots of the resultant $y^4 - 4y^2 - 1 = 0$ we can find the y-coordinates of the solutions to $f = g = 0$.

[Draw picture of circle of radius 2, the hyperbola $xy = 1$, and four horizontal lines at the intersection points]

In this example we actually have equalities $V(f,g) = V(\mathrm{Res}(f,g), f) = V(\mathrm{Res}(f,g), g)$.

1.3.2 Proof of the geometric sieve

Lemma 1.13 ([Bha14], slide 160)**.** *Let B be a compact region in $\mathbb{R}^n$ having finite measure, and let Y be any closed subscheme of $\mathbb{A}^n_{\mathbb{Z}}$ of codimension $k \geq 1$. Then*

$$\#\{a \in rB \cap Y \cap \mathbb{Z}^n\} = O(r^{n-k})$$

where the implied constant depends only on B and on Y.

We will give an elementary proof using resultants. Later we'll see how this bound can be improved using the large sieve.

Proof. The proof is by induction on n.

Without loss of generality, we may assume Y is the vanishing locus of polynomials $f_1, \ldots, f_k \in \mathbb{Z}[x_1, \ldots, x_n]$ since every irreducible component of Y is contained in such an intersection.

By the lemma, we may assume $f_1, \ldots, f_{k-1}$ are independent of x_n. If f_k is also independent of x_n then the result follows by induction.[2]

Let $h(x_1, \ldots, x_{n-1})$ be the leading coefficient of f_k as a polynomial in x_n. We may assume h is not identically zero on Y.

Let $\pi \colon \mathbb{A}^n \to \mathbb{A}^{n-1}$ be the projection map to the first $n-1$ coordinates. Then $\pi(Y \cap \{h = 0\}) = V(f_1, \ldots, f_{k-1}, h)$ has codimension k in $\mathbb{A}^{n-1}$, so by induction there are at most $O(r^{(n-1)-k})$ possible choices of $(a_1, \ldots, a_{n-1})$. There are r choices for a_n so the number of $a \in rB \cap Y \cap \mathbb{Z}^n$ for which $h(a) = 0$ is $O(r^{n-k})$.

Meanwhile for any fixed $a_1, \ldots, a_{n-1}$ for which $h(a) \neq 0$, there are at most $\deg_{x_n} f_k$ many values of a_n for which $f_k(x_1, \ldots, x_n) = 0$. The number of such $a_1, \ldots, a_{n-1}$ which extend to a point $a \in rB \cap Y \cap \mathbb{Z}^n$ is at most $O(r^{(n-1)-(k-1)}) = O(r^{n-k})$ by induction applied to the variety $V(f_1, \ldots, f_{k-1})$. □

The elementary proof of the last lemma only eliminated one variable from the presentation of the variety. In fact, the points on the variety are determined up to finitely many choices by a well-chosen set of $\dim Y$ coordinates, by Noether's normalization lemma. This proves the lemma immediately.

[2] Get $O(r^{(n-1)-k})$ by induction, and another r from the free choice of x_n.

Now we prove the geometric sieve in general.

Theorem 1.14 ([Bha14], slide 159)**.** *Fix an integer $2 \leq k \leq n$. Let B be a compact region in $\mathbb{R}^n$ having finite measure, and let Y be any closed subvariety of $\mathbb{A}^n_{\mathbb{Q}}$ whose irreducible components have codimension at least k. Let r and M be positive real numbers. Then as r and M go to infinity, possibly independently, we have that*

$$\#\{a \in rB \cap \mathbb{Z}^n \mid a \pmod p \in Y(\mathbb{F}_p) \textit{ for some prime } p > M\} \\ = O\left(\frac{r^n}{M^{k-1}\log M} + r^{n-k+1}\right)$$

where the implied constant depends only on B and on Y.

Since the number of lattice points $a \in rB \cap \mathbb{Z}^n$ which are in $Y(\mathbb{Z})$ is $O(r^{n-k})$ by the lemma, the bound is only really concerned with lattice points which are not globally on Y. For such points, we actually prove a slight strengthening of the theorem:

$$\#\{(a,p) \ : \ a \in rB \cap \mathbb{Z}^n, \ a \notin Y(\mathbb{Z}), \ a \pmod p \in Y(\mathbb{F}_p) \text{ for some prime } p > M\} \\ = O\left(\frac{r^n}{M^{k-1}\log M} + r^{n-k+1}\right).$$

We will split the left-hand set into two subsets depending on whether $p \leq r$ or $p > r$. These cases correspond to the two summands in the bound, respectively.

For those pairs (a,p) with $p \leq r$, the lattice points with a given reduction mod p are equidistributed in the r-box, so the density is determined by the mod p density which is bounded by the Lang–Weil estimate.

When the modulus p is larger than the sidelength r of the box, we will use induction on the number of variables. The elimination theory shows that the coordinate projection of Y onto the subvariety cut out by resultants is generically finite. On the open subset where the map is finite, the last coordinate is determined up to $O(1)$ possibilities, so using the lemma from last time we get a bound of the form $O(r^{(n-1)-(k-1)})r = O(r^{n-k+1})$. Meanwhile the locus where the map has positive dimensional fibers is addressed by induction since it involves fewer variables.

Remark 1.15. Note that the bound becomes trivial for large M, namely the left-hand set becomes empty once $M \gg r^d$ where d is the minimal degree of any bounding hypersurface in $\mathbb{A}^n_{\mathbb{Q}}$ for Y, for the trivial reason that a nonzero integer cannot be divisible by a larger prime.

So the primary regime of interest are those pairs (a, p) with $r \ll p \ll r^d$.

Proof. Suppose M is large enough so that the reduction of $Y \pmod{p}$ is well-defined and has codimension k in $\mathbb{A}^n_{\mathbb{F}_p}$ for any $p > M$.

First we bound the subset of pairs (a, p) satisfying $p \leq r$. Since $\#Y(\mathbb{F}_p) = O(p^{n-k})$ by Lang–Weil and rB can be covered by $O((r/p)^n)$ boxes of sidelength p, it follows that the number of $a \in rB \cap \mathbb{Z}^n$ such that $a \pmod{p} \in Y(\mathbb{F}_p)$ is $O(p^{n-k})O((r/p)^n) = O(r^n/p^k)$. Summing this over p with $M < p \leq r$ obtains

$$\begin{aligned}\#\{(a,p) \,:\, a \in rB \cap \mathbb{Z}^n,\ a \pmod{p} \in Y(\mathbb{F}_p),\ M < p \leq r\} \\ = \sum_{M<p\leq r} O(r^n/p^k) \ll r^n \sum_{m=M+1}^{\infty} m^{-k} = O\left(\frac{r^n}{M^{k-1}}\right).\end{aligned}$$

Note that in the last equality we used that $k \geq 2$. Being less sloppy one can get an additional $\log M$ in the denominator.

Now we bound those pairs (a, p) with $p > r$. Assume without loss of generality that Y is irreducible and has codimension k. We will prove the following stronger bound by induction on n:

$$\#\{(a,p) \,:\, a \in rB \cap \mathbb{Z}^n,\ p > r,\ a \notin Y(\mathbb{Z}),\ a \pmod{p} \in Y(\mathbb{F}_p)\} = O(r^{n-k+1}).$$

As in the proof of the lemma from last time, we may use resultants to suppose that Y is an irreducible component of a subvariety of the form

$$Y \subset V(f_1, \ldots, f_{k-1}, f_k)$$

where $f_1, \ldots, f_{k-1}$ do not involve the variable x_n, and the leading term h of f_k as a polynomial in x_n does not vanish identically on Y.

The base case is when $n = k = 2$. We may suppose $Y = \{0\}$ in $\mathbb{A}^2_{\mathbb{Q}}$, and want to show that $\#\{(a,p) \,:\, a \in rB \cap \mathbb{Z}^2,\ p > r,\ a \neq 0,\ a \equiv 0 \pmod{p}\} = O(r)$. This is trivially satisfied because the left-hand set has only $O(1)$ many elements.

Now suppose $n \geq 3$. Let Y_{k-1} denote the irreducible component of $V(f_1, \ldots, f_{k-1}) \subset \mathbb{A}^n_{\mathbb{Q}}$ which contains Y, and let Z denote the union of irreducible components of $V(f_1, \ldots, f_{k-1}, h) \subset \mathbb{A}^n_{\mathbb{Q}}$ which meet $Y \cap \{h = 0\}$. Then Y_{k-1} has codimension $k - 1$ and Z has codimension k

(using that $h|_Y \not\equiv 0$). The set we are bounding is bounded by three larger sets:

$$\begin{aligned}
&\{(a,p) \,:\, a \in rB \cap \mathbb{Z}^n,\ p > r,\ a \notin Y(\mathbb{Z}),\ a \pmod{p} \in Y(\mathbb{F}_p)\}\\
\subseteq\ &\{(a,p) \,:\, a \in rB \cap \mathbb{Z}^n,\ p > r,\ a \in Y_{k-1}(\mathbb{Z}),\ f_k(a) \neq 0,\ f_k(a) \equiv 0 \pmod{p}\} \cup\\
&\{(a,p) \,:\, a \in rB \cap \mathbb{Z}^n,\ p > r,\ a \notin Y_{k-1}(\mathbb{Z}),\ a \pmod{p} \in Z(\mathbb{F}_p)\} \cup\\
&\{(a,p) \,:\, a \in rB \cap \mathbb{Z}^n,\ p > r,\ a \notin Y_{k-1}(\mathbb{Z}),\ a \pmod{p} \in Y(\mathbb{F}_p),\ h(a) \not\equiv 0 \pmod{p}\}.
\end{aligned}$$

(The assumption that $p > r$ will only become relevant for the last set.)

For the first larger set, there are $O(r^{(n-1)-(k-1)})$ possibilities for the first $n-1$ coordinates by the lemma from last time, and then r choices for the last coordinate. Since $f_k(a)$ is not zero and $O(r^{O(1)})$, it has $O(1)$ many prime factors greater than r, so the number of pairs in the first set is bounded by $O(r^{(n-1)-(k-1)})rO(1) = O(r^{n-k+1})$.

For the second larger set, since $a \notin Y_{k-1}(\mathbb{Z})$ it also cannot be in $Z(\mathbb{Z})$ as $Z \subset Y_{k-1}$. We may regard Z as a subvariety of $\mathbb{A}^{n-1}_{\mathbb{Q}}$ since its k defining equations do not involve x_n, in which case the induction hypothesis gives us that the number of possibilities for the first $n-1$ coordinates is $O(r^{(n-1)-k+1})$. Multiplying this by r choices for the last coordinate obtains the desired bound.

Finally for the third larger set, by the induction hypothesis applied to Y_{k-1}, the number of choices for $b = (a_1, \ldots, a_{n-1})$ and p is at most $O(r^{(n-1)-(k-1)+1})$. Given such a pair (b,p), the number of choices for the last coordinate a_n is bounded by the degree of h. Since $p > r$ and $a_n = O(r)$, this means that in fact a_n is determined up to $O(1)$ possibilities. So the total number of pairs (a,p) in the third set is $O(r^{(n-1)-(k-1)+1})O(1) = O(r^{n-k+1})$. □

Remark 1.16. We have faithfully followed Bhargava's proof of the geometric sieve, but we note that like Lemma 1.13, the proof of the geometric sieve becomes somewhat easier if we use Noether normalization in place of resultants: since the projection map is finite and not just generically finite, there is no need to bound the second set (the "non-monic locus").

Later on in the course we will see some applications of the geometric sieve. For now we turn to improving the "trivial bound" given by Lemma 1.13.

2 The large sieve

We take a detour from squarefree values of polynomials to discuss the *large sieve*, a popular and useful sieve with many variants and applications. We have followed [CM06] for our discussion of the large sieve inequality.

2.1 The large sieve inequality

The large sieve inequality was introduced by Linnik in 1941 and subsequently developed by Rényi, Roth, Bombieri, Davenport–Halberstam, Gallagher, Montgomery–Vaughan, Selberg, Iwaniec, and others.

Linnik originally applied the large sieve to study the size of the least quadratic non-residue $n_p \pmod{p}$. Vinogradov conjectured that $n_p = O(p^\varepsilon)$, and one can show that $n_p = O(\log^2 p)$ assuming the generalized Riemann hypothesis. Using the large sieve, Linnik proved that the number of primes $p \leq x$ for which $n_p > p^\varepsilon$ is $O(\log \log x)$.

We now state the *large sieve inequality*. Let $S(x)$ be a trigonometric polynomial:

$$S(x) = \sum_{n=1}^{N} a_n e^{2\pi i n x}$$

where N is a positive integer and $a_1, \dots, a_N$ are arbitrary complex numbers normalized so that

$$\sum_{n=1}^{N} |a_n|^2 = 1.$$

The large sieve inequality is a bound for $|S(x)|^2$ when sampled over an arbitrary set of *distinct* elements $x_1, \dots, x_R$ of $\mathbb{R}/\mathbb{Z}$.

The Cauchy–Schwartz inequality implies that $\sum_{r=1}^{R} |S(x_r)|^2 \leq RN$. This is the sharpest bound possible for *arbitrary* $x_1, \dots, x_R$. Let

$$\delta = \min_{r \neq s} \|x_r - x_s\|$$

where $\|x\|$ denotes the distance of x to the nearest integer. We are interested in bounds which improve as δ grows.

Theorem 2.1 (The large sieve inequality). *Let $x_1, \ldots, x_R \in \mathbb{R}/\mathbb{Z}$ be distinct and at least δ apart from one another. Then*

$$\sum_{r=1}^{R} |S(x_r)|^2 \leq \Delta(N, \delta)$$

where $\Delta(N, \delta)$ is bounded from above by some explicit function of N and δ:

- $\pi N + \delta^{-1}$ *(Gallagher 1967)*
- $2\max(N, \delta^{-1})$ *(Bombieri–Davenport 1968)*
- $N + 2\delta^{-1}$ *(Bombieri 1971)*
- $N + \delta^{-1}$ *(Montgomery–Vaughan 1973).*

Remark 2.2. Bombieri–Davenport 1968 give examples in which $\Delta(N, \delta) = N + \delta^{-1} - 1$. [Evertse claims that Selberg actually showed the large sieve inequality with this Δ.] In 1973 Gallagher used his version of the large sieve inequality to prove that $O(H^{n-1/2+\varepsilon})$ is a valid upper bound for the van der Waerden problem for monic degree n integral polynomials.

Surprisingly, the large sieve inequality can be regarded as a manifestation of a basic fact from linear algebra: the norm of a bounded map $T\colon V \to W$ of normed linear spaces is equal to the norm of its adjoint $T^*\colon W^* \to V^*$:

$$\|T\| = \sup_{\|v\| \leq 1} \|Tv\| = \sup_{\|w\| \leq 1} \|T^* w\| = \|T^*\|.$$

This observation is sometimes called the "duality principle".

2.2 The large sieve

The large sieve inequality does not apparently match our concept of a sieve. By applying the large sieve inequality sampled at *Farey fractions*,[3] we can obtain the *large sieve* which does fit into our concept of a sieve.

This choice of sampling exploits the cancellation provided by *Ramanujan sums*, a particular type of exponential sum. See [CM06, §8.2] for more details on the derivation of the large sieve from the large sieve inequality.

[3] The set of all rational numbers in the real interval $[0, 1]$ of bounded height.

We will follow [Ser97] closely for our discussion of the large sieve. Let K be a number field with ring of integers O_K, and let Λ be a torsion free finitely generated O_K-module of rank n. Choose a norm $|\cdot|$ on $\Lambda_{\mathbb{R}} = \Lambda \otimes \mathbb{R}$.

For each prime ideal $\mathfrak{p}$ of O_K, let $\omega_{\mathfrak{p}}$ be a real number in $[0,1]$.

Let $r \geq 1$ and $Q > 0$ be real numbers.

We want to bound the size of a subset X of Λ satisfying the following local constraints:

1. The set X is contained in a ball of radius r, i.e. there is some $x_0 \in \Lambda_{\mathbb{R}}$ such that $|x - x_0| < r$ for every $x \in X$.
2. For every $\mathfrak{p}$ with $N(\mathfrak{p}) \leq Q$, the reduction $X_{\mathfrak{p}}$ of X in $\Lambda/\Lambda\mathfrak{p}$ satisfies

$$\#X_{\mathfrak{p}} \leq (1 - \omega_{\mathfrak{p}}) \cdot \#(\Lambda/\mathfrak{p}\Lambda).$$

The second assumption means that a proportion $\omega_{\mathfrak{p}}$ of the residue classes modulo $\mathfrak{p}$ of $\Lambda/\Lambda\mathfrak{p}$ have been "sieved out", and are entirely missing from X.

Theorem 2.3. *We have the bound*

$$\#X = O(\sup(r^{n[K:\mathbb{Q}]}, Q^{2n})/L(Q))$$

where

$$L(Q) = \sum_{I} \prod_{\mathfrak{p}|I} \frac{\omega_{\mathfrak{p}}}{1 - \omega_{\mathfrak{p}}}$$

and the sum is over squarefree ideals $I \subset O_K$ of norm $\leq Q$. The implied constant depends only on K, Λ, and the chosen norm.

Remark 2.4. The implied constant may be made explicit: it is 2^n for $K = \mathbb{Q}$, $\Lambda = \mathbb{Z}^n$ and $|\cdot|$ the sup norm.

Remarks on $L(Q)$: The quantity $L(Q)$ may be regarded as density-like. Consider the regime $Q^2 \approx r^{[K:\mathbb{Q}]}$, corresponding to only using the congruence constraints for O_K-sublattices of Λ with root discriminant $\leq r$. For instance, if $\omega_{\mathfrak{p}} = N(\mathfrak{p})^{-k}$ $(k \geq 1)$, then

$$L(Q) = \sum_{I \text{ sq.f}} \prod_{\mathfrak{p}|I} (N(\mathfrak{p})^{-k} + N(\mathfrak{p})^{-2k} + \cdots) = \sum_{I : N(I^{rad}) \leq Q} N(I)^{-k} \xrightarrow{r \to \infty} \zeta_K(k)$$

and then $r^{n[K:\mathbb{Q}]}/\zeta_K(k)$ is the leading term, which is sharp.

However one of the special features of the large sieve is that $\omega_{\mathfrak{p}}$ may be as large as a positive constant *that is independent of* $\mathfrak{p}$. We will see that this is the case for thin sets. When this occurs, $L(Q)$ will go to infinity with Q, and this will lead to power savings. In fact we will show that $L(Q) \gg Q/\log Q$.

Fourier analytic interpretation: As we have seen earlier in the course, the problem of bounding the size of a finite subset of lattice points $X \subset \Lambda$ can be studied using (abelian) harmonic analysis on the compact torus $T = \Lambda^\vee_{\mathbb{R}}/\Lambda^\vee$.

The basic idea is that Λ parametrizes the unitary characters $\chi_\lambda : T \to \mathbb{R}/\mathbb{Z}$ of T (where $\lambda \in \Lambda$), and properties of X are reflected in the properties of the function

$$f = \widehat{1_X} = \sum_{\lambda \in X} \chi_\lambda.$$

For instance, $f(0) = \widehat{1_X}(0) = \#X$, and the size of f away from zero is a measure of equidistribution of X. The Dirac delta function $\delta = \sum_{\lambda\in\Lambda} \chi_\lambda$ is the extreme example.

In terms of f, the first hypothesis says that the Fourier coefficients of f vanish outside a ball of radius r. By duality, the quotient lattice $\Lambda/\mathfrak{p}\Lambda$ is associated to the subgroup $T_{\mathfrak{p}}$ of $\mathfrak{p}$-torsion points of T. The second hypothesis says that at most a proportion of $1 - \omega_{\mathfrak{p}}$ of the Fourier coefficients of f restricted to $T_{\mathfrak{p}}$ are nonzero.

We now apply the large sieve to bound the number of integer points of bounded height in thin sets.

3 Thin sets

The following useful concept is due to Lang and Serre.

A subset of k-points of a variety V defined over a field k is called thin if it can be covered by a finite union of sets of the form:

- (type I) $C(k)$ for a proper Zariski-closed subset $C \subset V$, or
- (type II) $\pi(W(k))$ for a geometrically irreducible variety W defined over k and a generically finite dominant map $\pi\colon W \to V$ of degree ≥ 2.

(Type I sets are "small"; Type II sets are "sparse".) If $V(k)$ is not a thin set, then V is called Hilbertian (or Hilbert type). Hilbertian varieties may be regarded as having "many" k-rational points in the sense that $V(k)$ is Zariski dense and is not sparse.

Remark 3.1. One can show the property of being Hilbertian is a birational property.

Many Diophantine problems come down to bounding the number of rational or integral points of bounded height in a thin set.

For instance, in the van der Waerden problem on the space $V = \mathbb{A}^n$ of degree n monic polynomials, the subset of polynomials in $V(\mathbb{Z})$ (or $V(\mathbb{Q})$) with Galois group $G \neq S_n$ is a thin set. (Indeed they come from rational points on another variety via the natural quotient map $\pi \colon W = \mathbb{A}^n/G \to \mathbb{A}^n/S_n \cong V$.) Van der Waerden's conjecture is that this thin set has at most $O(r^{n-1})$ points of height $\leq r$.

The large sieve can be used to produce general bounds for the number of rational/integral points in a thin set of bounded height. The idea is that for an affine variety Y of dimension d, one may choose d linear coordinates $x_1, \ldots, x_d \in \mathcal{O}(Y)$ so that the projection map $\pi = (x_1, \ldots, x_d) : Y \to \mathbb{A}^d$ is finite. If Y is *nonlinear*, then π will have degree ≥ 2. This reduces the problem of bounding integer points in a thin set of bounded height in an *abstract variety* to bounding a thin set A of lattice points of bounded height in *affine space*.

Let A be a thin subset of O_K^d.

Theorem 3.2 (S. Cohen)**.** *$\#\{a \in A : |a| < r\} = O(r^{(d-1/2)[K:\mathbb{Q}]} \log r)$.*

Remark 3.3. [Ser97] improves this to $\log^\gamma r$ in place of $\log r$ for some $\gamma < 1$.

Corollary 3.4. *Let K be a number field. The number of monic degree d polynomials with coefficients in O_K, Galois group not S_d, and height $\leq r$ is $O(r^{(d-1/2)[K:\mathbb{Q}]} \log^\gamma r)$.*

(A possible height is $|t^d + a_1 t^{d-1} + \cdots + a_d| = \max_{k, \sigma \colon K \to \mathbb{C}} |\sigma a_k|$.)

We will show, using an amplification of Lang–Weil, that the reductions modulo p of a thin set are constrained a priori, with $\omega_\mathfrak{p}$ which are *independent of* $\mathfrak{p}$. This provides the necessary data to apply the large sieve and get a power savings to prove this theorem.

Let V be a geometrically irreducible variety over a finite field $\mathbb{F}_v$. Recall the Lang–Weil estimate:

$$\#V(\mathbb{F}_v) = (Nv)^{\dim V} + O((Nv)^{\dim V - \frac{1}{2}}).$$

This estimate suffices to bound the image of reduction of a Type I set mod v, but for type II thin sets we will require a more precise result.

Let $\pi\colon W \to V$ be a finite étale morphism of geometrically irreducible smooth varieties over $\mathbb{F}_v$ with $\deg \pi = m \geq 2$.

Theorem 3.5 (Lang–Weil for type II thin sets)**.** *If the Galois closure of W/V is geometrically irreducible, then*

$$\#\pi(W(\mathbb{F}_v)) \leq \left(\tfrac{d_m - 1}{d_m}\right)(Nv)^{\dim V} + O((Nv)^{\dim V - 1/2})$$

where d_m is $m(m-2)!$.

The important feature of this estimate is that the leading constant is less than 1 and independent of v.

Proof. Let $W^{\mathrm{gal}} \to W \to V$ be the Galois closure of W/V. Since it is geometrically irreducible by assumption, we can apply Lang–Weil to $|W^{\mathrm{gal}}(\mathbb{F}_v)|$ and also the Galois group of W/V acts freely on $W^{\mathrm{gal}}(\mathbb{F}_v)$.

(If W^{gal} is geometrically irreducible, then $W^{\mathrm{gal}}_{\overline{\mathbb{F}_v}}$ is also the Galois closure of $W_{\overline{\mathbb{F}_v}}/V_{\overline{\mathbb{F}_v}}$. This shows that the Galois group of $W_{\overline{\mathbb{F}_v}}/V_{\overline{\mathbb{F}_v}}$ (the geometric monodromy group) is equal to the Galois group of W/V. The geometric monodromy group acts freely on $W^{\mathrm{gal}}_{\overline{\mathbb{F}_v}}$ (decomposition groups must be trivial), so the Galois group of W/V also acts freely on W^{gal}.)

Write $W(\mathbb{F}_v) = A \sqcup B$, where A is the image of $W^{\mathrm{gal}}(\mathbb{F}_v)$. Each point in $\pi(A)$ has precisely m points of A lying over it. Then

$$\#\pi(W(\mathbb{F}_v)) \leq \#\pi(A) + \#\pi(B) \leq \tfrac{1}{m}\#A + \#B = \#W(\mathbb{F}_v) - \left(1 - \tfrac{1}{m}\right)\#A.$$

Putting $W^{\mathrm{gal}}(\mathbb{F}_v) = [W^{\mathrm{gal}} : W] \cdot \#A$ into the above obtains

$$\begin{aligned}\#\pi(W(\mathbb{F}_v)) &\leq \#W(\mathbb{F}_v) - \left(1 - \tfrac{1}{m}\right)[W^{\mathrm{gal}} : W]^{-1} W^{\mathrm{gal}}(\mathbb{F}_v) \\ &= \#W(\mathbb{F}_v) - (1 - \tfrac{1}{m})[W^{\mathrm{gal}} : W]^{-1}((Nv)^{\dim V} + O((Nv)^{\dim V - \frac{1}{2}})) \\ &= c(Nv)^{\dim V} + O((Nv)^{\dim V - \frac{1}{2}})\end{aligned}$$

where $c = 1 - (1 - \frac{1}{m})[W^{\mathrm{gal}} : W]^{-1} = 1 - (1 - \frac{1}{m})\frac{[W:V]}{[W^{\mathrm{gal}}:V]} \leq 1 - (1 - \frac{1}{m})\frac{m}{m!}$.

Then use that $1 - (1 - \frac{1}{m})\frac{m}{m!} = \frac{d_m - 1}{d_m}$. □

3.1 Proof of Cohen's theorem

Now we use Theorem 3.5 to prove Theorem 3.2.

Proof of Theorem 3.2. If A is a Type I thin set, then one easily proves the required bound by induction on the dimension. So we reduce to proving the bound for a set of the form $A \cap O_K^d$ where A is the image of the K-points of W under $\pi \colon W \to V$, a generically finite dominant map with degree ≥ 2 where W is geometrically irreducible.

We apply the large sieve to the subset $X = \{a \in A \cap O_K^d : |a| < r\}$ of the lattice O_K^d in the regime $Q^2 \approx r^d$:

$$\#\{a \in A : |a| < r\} \leq c_{K,d} r^{d[K:\mathbb{Q}]}/L(Q)$$

where

$$L(Q) = \sum_{\substack{N(I) \leq Q \\ I \text{ sq.f}}} \prod_{\mathfrak{p}|I} \frac{\omega_\mathfrak{p}}{1-\omega_\mathfrak{p}}$$

and

$$1 - \omega_\mathfrak{p} = \frac{|A \pmod{\mathfrak{p}}|}{N\mathfrak{p}^d}.$$

Let K_π be the maximal finite extension of K inside the Galois closure W^{gal} of W/V. If $\mathfrak{p}$ is split in K_π, then the reduction of W^{gal} modulo $\mathfrak{p}$ will be geometrically irreducible. Thus by Lang–Weil for Type II thin sets (Theorem 3.5), there is a constant $0 < c < 1$ such that $|A \pmod{\mathfrak{p}}| \leq cN\mathfrak{p}^d$ for all primes $\mathfrak{p}$ which are split in K_π. In particular, $1 - \omega_\mathfrak{p} \leq c < 1$ where c is independent of $\mathfrak{p}$ for such primes.

It only remains to show that

Lemma 3.6. *$L(Q) \gg Q/\log Q$.*

For this lower bound, it suffices to only keep the *prime* ideals in the sum defining $L(Q)$:

$$L(Q) \geq \sum_{N\mathfrak{p} \leq Q} \frac{\omega_\mathfrak{p}}{1-\omega_\mathfrak{p}}.$$

Now observe that

$$\sum_{N\mathfrak{p} \leq Q} \frac{\omega_\mathfrak{p}}{1-\omega_\mathfrak{p}} \gg \sum_{\substack{N\mathfrak{p} \leq Q \\ \mathfrak{p} \text{ splits in } K_\pi}} 1$$

By the prime number theorem,

$$\sum_{\substack{N\mathfrak{p}\leq Q \\ \mathfrak{p} \text{ splits in } K_\pi}} 1 \sim \frac{1}{[K_\pi : K]}\frac{Q}{\log Q}.$$

This completes the proof. □

3.2 p-adic and mod p densities of thin sets

Theorem 3.5 has some interesting consequences for the reduction of a thin set modulo primes.

Corollary 3.7. *If $N\mathfrak{p}$ is large and $\mathfrak{p}$ splits completely in K_π, then $A \pmod{\mathfrak{p}} \neq \mathbb{A}^n(\mathbb{F}_\mathfrak{p})$.*

The mod p density of $A \pmod{p}$ is closely related to p-adic density of A.

Definition 3.8 (WWA)**.** Let S be a finite set of places of a number field K. A variety V over a number field K is said to satisfy weak approximation with respect to S if the image of $V(K) \to \prod_{v\in S} V(K_v)$ is topologically dense. If V satisfies weak approximation with respect to all such S than we say V satisfies weak approximation; if there exists a finite set S_0 of places of K such that V satisfies weak approximation with respect to all finite sets of places S with $S \cap S_0 = \varnothing$ then we say V satisfies weak weak approximation.

Example 3.9. Any K-rational variety satisfies weak approximation. Any algebraic torus satisfies WWA but not necessarily WA.

Theorem 3.10 (Ekedahl, Colliot-Thélène)**.** *If $A \subset V(\mathbb{Q})$ is thin, then A fails to be dense in $V(\mathbb{Q}_v)$ for all v in a subset of primes with positive density. In particular, WWA implies Hilbertian.*

Proof. Part I, reduction to residue fields. Either type of thin set is covered by $\pi(W(\mathbb{Q}_v))$ for some geometrically irreducible variety W and proper morphism $\pi\colon W \to V$. By replacing W and V with open subsets, we can suppose W and V are regular. By 'spreading out' we can define π, W, V over a nonempty open subset U of $\operatorname{Spec}\mathbb{Z}$, such that W and V are smooth over U.

We now show that $\pi(W(\mathbb{F}_v)) \subset V(\mathbb{F}_v)$ not dense $\implies$ $\pi(W(\mathbb{Q}_v)) \subset V(\mathbb{Q}_v)$ not dense.

Let $v \in U$. By smoothness, $\pi(W(\mathbb{F}_v)) \neq V(\mathbb{F}_v) \implies \pi(W(\mathbb{Z}_v)) \neq V(\mathbb{Z}_v)$.

By the valuative criterion for properness applied to π, $z \in V(\mathbb{Z}_v)$ if and only if $\pi^{-1}(z) \subset W(\mathbb{Z}_v)$. So $\pi(W(\mathbb{Z}_v)) \neq V(\mathbb{Z}_v) \implies \pi(W(\mathbb{Q}_v)) \neq V(\mathbb{Q}_v)$.

As π induces a topologically closed map on $\mathbb{Q}_v$-points, $\pi(W(\mathbb{Q}_v)) \neq V(\mathbb{Q}_v) \implies \pi(W(\mathbb{Q}_v)) \subset V(\mathbb{Q}_v)$ not dense.

We've reduced to showing $\pi(W(\mathbb{F}_v)) \neq V(\mathbb{F}_v)$ for a positive density set of v. For this we will use an amplification of Lang–Weil for thin sets.

Part II, apply Lang–Weil and Chebotarev density. Recall we must show $\pi(W(\mathbb{F}_v)) \neq V(\mathbb{F}_v)$ for a positive density set of v.

By replacing W, V, U with open subsets, we may assume π is finite étale, and that W_v, V_v are geometrically irreducible for any $v \in U$ (e.g. [EGA IV$_3$, 9.7.8]).

If the Galois closure of $W_v \to V_v$ is geometrically irreducible, the needed result follows from Lang–Weil for type II thin sets.

More generally, the Galois closure of $W_v \to V_v$ is geometrically irreducible if and only if v is totally split in k_π, the algebraic closure of $\mathbb{Q}$ in the Galois closure of $Q(W)/Q(V)$.

By Chebotarev's density theorem, this occurs for all $v \in U$ on a positive density subset. □

Remark 3.11. This theorem has consequences for the inverse Galois problem. Let $\pi\colon W \to V$ be a generically étale G-torsor of geometrically irreducible varieties defined over $\mathbb{Q}$. If V satisfies WWA, then there exists a Galois field extension of $\mathbb{Q}$ with Galois group G.

4 The density of squarefree values of invariant polynomials

We return to the problem of computing the density of squarefree values of invariant polynomials. Following [Bha14, §2], we outline axioms from which the correct density may be proven.

4.1 Hypotheses on invariant polynomials

Let V be a representation of an algebraic group G defined over $\mathbb{Z}$. Let f be an integer polynomial of degree d that is a relative invariant for the action of G on V and whose squarefree values we wish to extract. Let m be the dimension of V. Let G^1 denote the kernel of the determinant map $G \to \mathbf{GL}(V) \to \mathbb{G}_m$.

[Write out six axioms.]

Remark 4.1. Condition 6(iii) has a typo, it should say: for each fixed k, every point of $V(\mathbb{Z})^{\text{gen}}$ with $g_v v \pmod p \in Y_k(\mathbb{F}_p)$ arises as $g_v v$ for some $V(\mathbb{Z})^{\text{gen}}$ at most c times up to $G(\mathbb{Z})$-equivalence, where c is an absolute constant.

Theorem 4.2. *If f, G, V satisfy these six conditions, then f takes the expected density of squarefree values.*

4.2 Application to number fields of degree ≤ 5

We will apply the preceding setup to polynomials arising in the arithmetic of rings over $\mathbb{Z}$ which are free of rank ≤ 5.

Let $f \in \{f_3, f_4, f_5\}$ denote the primitive integral polynomial that generates the ring of invariants for

1. the action of $\mathbf{SL}_2(\mathbb{C})$ on $\mathrm{Sym}_3(\mathbb{C}^2)$, the space of binary cubic forms over $\mathbb{C}$;
2. the action of $\mathbf{SL}_2 \times \mathbf{SL}_3(\mathbb{C})$ on $\mathbb{C}^2 \otimes \mathrm{Sym}_2(\mathbb{C}^3)$, the space of pairs of ternary quadratic forms over $\mathbb{C}$; or
3. the action of $\mathbf{SL}_4 \times \mathbf{SL}_5(\mathbb{C})$ on $\mathbb{C}^4 \otimes \wedge^2(\mathbb{C}^5)$, the space of quadruples of 5×5 skew-symmetric matrices over $\mathbb{C}$.

In each case, f is a polynomial of degree m in m variables where $m = 4, 12$ or 40, respectively. We will show that these three polynomials satisfy the preceding setup, and therefore have the expected density of squarefree values.

These three polynomials turn out to have the *same* expected density of squarefree values, given by

$$\prod_p (1 - c_p/p^{2m}) = \frac{2}{3}\zeta(2)^{-1}$$

where c_p is, as usual, the number of $x \in (\mathbb{Z}/p^2\mathbb{Z})^m$ satisfying $f(x) = 0$ in $\mathbb{Z}/p^2\mathbb{Z}$.

This theorem can be used to determine the density of S_n-number fields with squarefree discriminant for $n = 3, 4, 5$.

Theorem 4.3. *Let $n = 3, 4$ or 5 and let $N_n^{\mathrm{sqf}}(X)$ denote the number of isomorphism classes of number fields of degree n that have squarefree discriminant of absolute value less than X. Then*

$$N_n^{\mathrm{sqf}}(X) = \frac{r_2(S_n)}{3 \cdot n!}\zeta(2)^{-1} \cdot X + o(X)$$

where $r_2(S_n)$ denotes the number of 2-torsion elements in the symmetric group S_n.

4.3 Proof of Theorem 4.2

Let f, G, V be as in §4.1, satisfying the six conditions there. We begin by showing that f takes the correct density of squarefree values in a large scaling of the fundamental domain when we only sample the *generic* points, i.e.

$$\lim_{X\to\infty} \frac{\#\{x \in \mathcal{F}_X \cap V(\mathbb{Z})^{\mathrm{gen}} : f(x) \text{ squarefree}\}}{\#\{x \in \mathcal{F}_X \cap V(\mathbb{Z})^{\mathrm{gen}}\}} = \prod_p (1 - c_p/p^{2m}) \tag{1}$$

where c_p as before denotes the number of elements $x \in (\mathbb{Z}/p^2\mathbb{Z})^m$ satisfying $f(x) = 0$ in $\mathbb{Z}/p^2\mathbb{Z}$.

Compactly approximating the fundamental domain: First we define a compact approximation to $\mathcal{F}_X$ which will be used as the homogeneously expanding region in the geometric sieve. Let $\varepsilon > 0$ be a small parameter and choose a compact measurable subset

$$\mathcal{F}_1^{1-\varepsilon} \subset \mathcal{F}_1 \qquad \text{satisfying} \qquad \mathrm{Vol}(\mathcal{F}_1^{1-\varepsilon}) = (1-\varepsilon)\mathrm{Vol}(\mathcal{F}_1).$$

(That is, $\mathcal{F}_1^{1-\varepsilon}$ is obtained from $\mathcal{F}_1$ by cutting off the cusps of $\mathcal{F}_1$ sufficiently far out.) Set

$$\mathcal{F}_X^{1-\varepsilon} := X^{1/d} \cdot \mathcal{F}_1^{1-\varepsilon} \qquad \text{so that} \qquad \mathrm{Vol}(\mathcal{F}_X^{1-\varepsilon}) = (1-\varepsilon)\mathrm{Vol}(\mathcal{F}_X).$$

We need to estimate the error of counting lattice points with the compact approximation. As X grows, the volume of $\mathcal{F}_X^{1-\varepsilon}$ grows proportionally by $X^{m/d}$. Thus the number of lattice points in $V(\mathbb{Z})$ which lie in $\mathcal{F}_X^{1-\varepsilon}$ is $\mathrm{Vol}(\mathcal{F}_X^{1-\varepsilon}) + o(X^{m/d})$. By Condition 1 ("HIT"), the non-generic points in $V(\mathbb{Z})$ have density zero, and thus

$$\begin{aligned}|\mathcal{F}_X^{1-\varepsilon}\cap V(\mathbb{Z})^{\mathrm{gen}}| = |\mathcal{F}_X^{1-\varepsilon}\cap V(\mathbb{Z})| + o(X^{m/d}) &= \mathrm{Vol}(\mathcal{F}_X^{1-\varepsilon}) + o(X^{m/d})\\ &= (1-\varepsilon)\mathrm{Vol}(\mathcal{F}_1)X^{m/d} + o(X^{m/d}).\end{aligned}$$

With the help of Condition 5 ("CRT"), the same argument applied to a subset $S\subset V(\mathbb{Z})$ defined by finitely many congruence conditions shows that

$$|\mathcal{F}_X^{1-\varepsilon}\cap S^{\mathrm{gen}}| = (1-\varepsilon)\mathrm{Vol}(\mathcal{F}_1)X^{m/d}\prod_p \mu_p(S) + o(X^{m/d}).$$

Meanwhile, Condition 5 ("CRT") also estimates number of the generic points of S in the entire (non-compact) fundamental domain $\mathcal{F}_X$ to be

$$|\mathcal{F}_X\cap S^{\mathrm{gen}}| = \mathrm{Vol}(\mathcal{F}_1)X^{m/d}\prod_p \mu_p(S) + o(X^{m/d}).$$

This shows that the error of using the compact approximation is

$$|(\mathcal{F}_X\backslash\mathcal{F}_X^{1-\varepsilon})\cap S^{\mathrm{gen}}| = \varepsilon\mathrm{Vol}(\mathcal{F}_1)X^{m/d}\prod_p \mu_p(S) + o(X^{m/d}). \tag{2}$$

Proving the upper bound on the density: For each prime p let $S_p = \{v\in V(\mathbb{Z}) : p^2\nmid f(v)\}$ and set $S=\cap_p S_p$.

Since

$$\frac{|\mathcal{F}_X\cap\bigcap_{p\le M} S_p^{\mathrm{gen}}|}{X^{m/d}}$$

is a monotonically decreasing function of M,

$$\inf_{M>0}\frac{|\mathcal{F}_X\cap\bigcap_{p\le M} S_p^{\mathrm{gen}}|}{X^{m/d}} = \lim_{M\to\infty}\frac{|\mathcal{F}_X\cap\bigcap_{p\le M} S_p^{\mathrm{gen}}|}{X^{m/d}}.$$

Exercise: Show that for any doubly-indexed sequence $(\phi_{X,M})_{X,M>0}$ one has

$$\limsup_{X\to\infty}\inf_{M>0}\phi_{X,M}\le\inf_{M>0}\limsup_{X\to\infty}\phi_{X,M}.\quad\square$$

By Condition 5 (CRT) applied to the set $\bigcap_{p\leq M} S_p$, we have that

$$\left|\mathcal{F}_X \cap \bigcap_{p\leq M} S_p^{\text{gen}}\right| = \text{Vol}(\mathcal{F}_X)\cdot \prod_{p\leq M} \mu_p(S) + o(X^{m/d}).$$

(Note that this formula requires taking X to infinity *before* M, since we did not stipulate that the implied constant was independent of M.)

By Condition 4, $\text{Vol}(\mathcal{F}_X) = \text{Vol}(X^{1/d}\mathcal{F}_1) = X^{m/d}\text{Vol}(\mathcal{F}_1)$. Thus

$$\begin{aligned}\limsup_{X\to\infty} \frac{|\mathcal{F}_X\cap S^{\text{gen}}|}{X^{m/d}} = \limsup_{X\to\infty}\inf_{M>0} \frac{|\mathcal{F}_X\cap \bigcap_{p\leq M} S_p^{\text{gen}}|}{X^{m/d}} &\leq \inf_{M>0}\limsup_{X\to\infty} \frac{|\mathcal{F}_X\cap \bigcap_{p\leq M} S_p^{\text{gen}}|}{X^{m/d}} \\ &\leq \inf_{M>0} \text{Vol}(\mathcal{F}_1)\cdot \prod_{p\leq M}\mu_p(S) \\ &= \text{Vol}(\mathcal{F}_1)\cdot \prod_{p}\mu_p(S).\end{aligned}$$

Proving the lower bound on the density: For the lower bound, we'll prove that there are few generic points $v\in\mathcal{F}_X$ for which $f(v)$ is divisible by p^2 for large primes p. Let $W_p = V(\mathbb{Z})\backslash S_p \subset V(\mathbb{Z})$ denote the set of points v with $p^2|f(v)$. Observe that

$$\bigcap_{p\leq M} S_p \subset \left(S \cup \bigcup_{p>M} W_p\right)$$

and thus

$$\left|\mathcal{F}_X \cap \bigcap_{p\leq M} S_p^{\text{gen}}\right| \leq |\mathcal{F}_X\cap S^{\text{gen}}| + \left|\mathcal{F}_X\cap \bigcup_{p>M} W_p^{\text{gen}}\right|.$$

Lemma 4.4 (tail estimate)**.**

$$\left|\mathcal{F}_X\cap \bigcup_{p>M} W_p^{\text{gen}}\right| = O_\varepsilon(X^{m/d}/(M^{\min(\eta,1)}\log M) + X^{\frac{m-1}{d}}) + O(\varepsilon X^{m/d}) + o(X^{m/d})$$

where the implied constants are independent of M and X.

Remark 4.5. [Bha14] does not have the term $o(X^{m/d})$, but this error term comes up from Condition 5 when estimating the number of weak multiples of p^2 in $\mathcal{F}_X\cap V(\mathbb{Z})^{\text{gen}}$ with $M < p \leq X^{1/(2d)}$.

By the lemma,

$$\left|\mathcal{F}_X \cap \bigcap_{p\le M} S_p^{\mathrm{gen}}\right| \le |\mathcal{F}_X \cap S^{\mathrm{gen}}| + O_\varepsilon(X^{m/d}/(M^{\min(\eta,1)}\log M) + X^{\frac{m-1}{d}}) + O(\varepsilon X^{m/d}) + o(X^{m/d}).$$

Using Condition 5 again on the left-hand side, we have now

$$\begin{aligned}&\mathrm{Vol}(\mathcal{F}_X)\cdot\prod_{p\le M}\mu_p(S) \le \\ &\qquad |\mathcal{F}_X \cap S^{\mathrm{gen}}| + O_\varepsilon(X^{m/d}/(M^{\min(\eta,1)}\log M) + X^{\frac{m-1}{d}}) + O(\varepsilon X^{m/d}) + o(X^{m/d}).\end{aligned}$$

Dividing by $X^{m/d}$ and taking the limit infimum over X obtains

$$\mathrm{Vol}(\mathcal{F}_1)\cdot\prod_{p\le M}\mu_p(S) \le \liminf_{X\to\infty}\frac{|\mathcal{F}_X \cap S^{\mathrm{gen}}|}{X^{m/d}} + O_\varepsilon(1/(M^{\min(\eta,1)}\log M)) + O(\varepsilon).$$

Now take M to infinity, and then ε to zero to obtain the correct lower bound:

$$\mathrm{Vol}(\mathcal{F}_1)\cdot\prod_{p}\mu_p(S) \le \liminf_{X\to\infty}\frac{|\mathcal{F}_X \cap S^{\mathrm{gen}}|}{X^{m/d}}.$$

We have shown the correct lower and upper bounds, and thus

$$\lim_{X\to\infty}\frac{|\mathcal{F}_X \cap S^{\mathrm{gen}}|}{X^{m/d}\mathrm{Vol}(\mathcal{F}_1)} = \lim_{X\to\infty}\frac{|\mathcal{F}_X \cap S^{\mathrm{gen}}|}{\mathrm{Vol}(\mathcal{F}_X)} = \prod_p \mu_p(S).$$

We have shown that f has squarefree values with the correct density when we sample over *generic* points in large scalings of the fundamental domain. This concludes the proof of (1).

Now we return to the proof of the lemma.

Proof. Write $W_p^{\mathrm{gen}} = W_p^{(1)} \sqcup W_p^{(2)}$ where $W_p^{(1)}$ (resp. $W_p^{(2)}$) denotes the set of points where the discriminant is strongly (resp. weakly) a multiple of p^2. By Corollary 1.8, there is a subvariety Y of $\mathbb{A}^n_{\mathbb{Q}}$ of codimension two such that for all but finitely many primes p,

$$\{a \in V(\mathbb{Z}) \mid f \text{ is strongly a multiple of } p^2 \text{ at } a\} \subseteq \{a \in V(\mathbb{Z}) \mid a \pmod p \in Y(\mathbb{F}_p)\}.$$

Observe that

$$\begin{aligned}
&\left|\mathcal{F}_X \cap \left(\cup_{p>M} W_p^{(1)}\right)\right| \\
&\leq |\{a \in \mathcal{F}_X \cap V(\mathbb{Z}) : a \pmod p \in Y(\mathbb{F}_p) \text{ for some prime } p > M\}| \\
&\leq \left|\left\{a \in \mathcal{F}_X^{1-\varepsilon} \cap V(\mathbb{Z}) : a \pmod p \in Y(\mathbb{F}_p) \text{ for some prime } p > M\right\}\right| \\
&\quad + \left|\left\{a \in (\mathcal{F}_X \backslash \mathcal{F}_X^{1-\varepsilon}) \cap V(\mathbb{Z})\right\}\right| \\
&\leq \left|\left\{a \in \mathcal{F}_X^{1-\varepsilon} \cap V(\mathbb{Z}) : a \pmod p \in Y(\mathbb{F}_p) \text{ for some prime } p > M\right\}\right| \\
&\quad + \varepsilon \mathrm{Vol}(\mathcal{F}_X).
\end{aligned}$$

We apply the geometric sieve to the compact approximation $\mathcal{F}_1^{1-\varepsilon}$ with scaling parameter $r = X^{1/d}$ to obtain the bound

$$\begin{aligned}
&\left|\left\{a \in \mathcal{F}_X^{1-\varepsilon} \cap V(\mathbb{Z}) : a \pmod p \in Y(\mathbb{F}_p) \text{ for some prime } p > M\right\}\right| \\
&= O_\varepsilon\left(\frac{X^{m/d}}{M^{2-1}\log M} + (X^{1/d})^{m-2+1}\right) \\
&= O_\varepsilon\left(\frac{X^{m/d}}{M\log M} + X^{(m-1)/d}\right).
\end{aligned}$$

Combining these,

$$\left|\mathcal{F}_X \cap \left(\cup_{p>M} W_p^{(1)}\right)\right| = O_\varepsilon\left(\frac{X^{m/d}}{M\log M} + X^{(m-1)/d}\right) + O(\varepsilon X^{m/d}).$$

This proves the required bound for strong multiples.

For the weak multiples in $W_p^{(2)}$ for primes p in the range $M < p \leq X^{1/(2d)}$, observe that any $v \in W_p^{(2)}$ has $f(v)$ divisible by p^2 where $p^2 \leq X^{1/d}$. Such v which are also in the compact region $\mathcal{F}_X^{1-\varepsilon} = X^{1/d}\mathcal{F}_1^{1-\varepsilon}$ are determined by congruence conditions modulo p^2 where the modulus p^2 is smaller than the diameter $X^{1/d}$ of the bounding region. For each such p, the region $\mathcal{F}_X^{1-\varepsilon}$ is covered by $O((X^{1/d}/p^2)^m)$ many boxes of sidelength p^2, and each box contributes $c_p = \{a \in V(\mathbb{Z}/p^2\mathbb{Z}) : f(a) \equiv 0 \pmod{p^2}\}$.

We claim that

$$c_p = O(p^{2(m-2)}).$$

Indeed, suppose $a \in V(\mathbb{Z}/p^2\mathbb{Z})$ and $f(a) \equiv 0 \pmod p$.

If $f(x_1, a_2, \ldots, a_m)$, a polynomial in x_1, satisfies $\partial_1 f(a) \not\equiv 0 \pmod p$, then knowing the residue $a_1 \pmod p$ uniquely determines $a_1 \pmod{p^2}$ by Hensel's lemma. Thus, the points

$a \in V(\mathbb{Z}/p^2\mathbb{Z})$ for which $f(a) \equiv 0 \pmod{p}$ and $\partial_k f(a) \not\equiv 0 \pmod{p}$ for all k are determined by their reductions mod p, and there are $O(p^{m-1})$ such points in $V(\mathbb{Z}/p\mathbb{Z})$ by the Lang–Weil bound.

Meanwhile, the number of points $a \in V(\mathbb{Z}/p\mathbb{Z})$ for which $f(a) \equiv 0 \pmod{p}$ and $\partial_k f(a) \equiv 0 \pmod{p}$ for some k is $O(p^{m-2})$ since it is a finite union of subvarieties of codimension at least two by Condition 7. Each point of $V(\mathbb{Z}/p\mathbb{Z})$ has p^m lifts to $V(\mathbb{Z}/p\mathbb{Z})$, so we see that $c_p = O(p^{2(m-2)})$.

Thus

$$\#\{(v,p) : v \in \mathcal{F}_X^{1-\varepsilon} \cap W_p^{(2)}\} = \sum_{M < p \leq X^{1/(2d)}} O(X^{m/d}/p^2) = O\left(\frac{X^{m/d}}{M \log M}\right).$$

Recall our earlier error estimate (2) for generic points in the cusps:

$$|(\mathcal{F}_X \backslash \mathcal{F}_X^{1-\varepsilon}) \cap V(\mathbb{Z})^{\text{gen}}| = \varepsilon \text{Vol}(\mathcal{F}_1) X^{m/d} \prod_p \mu_p(S) + o(X^{m/d}).$$

This shows that

$$\begin{aligned}\#\{(v,p) : v \in \mathcal{F}_X \cap W_p^{(2)}\} &\leq O\left(\frac{X^{m/d}}{M \log M}\right) + |(\mathcal{F}_X \backslash \mathcal{F}_X^{1-\varepsilon}) \cap V(\mathbb{Z})^{\text{gen}}| \\ &= O\left(\frac{X^{m/d}}{M \log M}\right) + O(\varepsilon X^{m/d}) + o(X^{m/d}).\end{aligned}$$

Now we turn to the weak multiples in $W_p^{(2)}$ for primes p in the range $p > X^{1/(2d)}$ (congruence larger than the sidelength of the box). For this estimate we will use Condition 6. Write $W_p^{(2)} = \cup_{k=0}^m W_p^{(2)}(k)$ where $W_p^{(2)}(k)$ is the subset of $W_p^{(2)}$ having a given value of k in Condition 6(ii).

For such a k, let α denote the infimum of a over all $v \in W_p^{(2)}(k)$.

By Condition 6, there is an element $g \in G(\mathbb{Q})$ such that $gv \in V(\mathbb{Z})^{\text{gen}}$, $|I(gv)| = p^{-a}|I(v)| \leq X/p^{\alpha}$, and $gv \pmod{p}$ lies on $Y_k(\mathbb{F}_p)$. Furthermore, a given element of $V(\mathbb{Z})^{\text{gen}}$ which reduces mod p to a point on Y_k can only arise as gv for finitely many v up to $G(\mathbb{Z})$-equivalence by Condition 6(iii).

This shows that

$$N(W_p^{(2)}(k);X) = O(N(V(\mathbb{Z});X/p^\alpha)) = O((X/p^\alpha)^{m/d})$$

where the second inequality follows from Condition 5 ("CRT for generic points in the fund. domain").

If $k=0$ then we can sum this estimate over primes $p > M' = \max\{M, X^{1/(2d)}\}$ to get

$$\left|\mathcal{F}_X \cap \bigcup_{p>M} W_p^{(2)}(0)\right| = O(X^{m/d}/(M')^{\alpha(m/d)-1}) = O(X^{m/d}/(M^\eta \log M))$$

since $\alpha(m/d) - 1 \geq \eta > 0$ by assumption.

If $k \geq 1$, then we use the geometric sieve again with Condition 6:

$$N(\cup_{p>M'} W_p^{(2)}(k);X) = O(|\{v \in V(\mathbb{Z}) : v \in \mathcal{F}_{X/p^\alpha}, v \pmod{p} \in Y_k(\mathbb{F}_p) \text{ for some } p > M'\}|)$$

$$\begin{aligned}&= O(|\{v \in \mathcal{F}^{1-\varepsilon}_{X/M'^\alpha} \cap V(\mathbb{Z}) : v \pmod{p} \in Y_k(\mathbb{F}_p) \text{ for some } p > M'\}| + \varepsilon(X/M'^\alpha)^{m/d}))\\ &= O_\varepsilon((X/M'^\alpha)^{m/d}/(M'^{k-1}\log M') + (X/M'^\alpha)^{\frac{m-k+1}{d}}) + O(\varepsilon(X/M'^\alpha)^{m/d}).\end{aligned}$$

Summing this over $k \in \{1,\ldots,m\}$ proves the claimed bound. □

We have shown that

$$\lim_{X\to\infty} \frac{\#\{x \in \mathcal{F}_X \cap V(\mathbb{Z})^{\text{gen}} : f(x) \text{ squarefree}\}}{\#\{x \in \mathcal{F}_X \cap V(\mathbb{Z})^{\text{gen}}\}} = \prod_p (1 - c_p/p^{2m}).$$

In other words, the correct density is obtained on generic points in a fundamental domain for $G(\mathbb{Z})$ acting on $V(\mathbb{R})$.

Now we would like to prove the correct density is obtained in a large ball. Let $B_N = [-N,N]^m \subset V(\mathbb{R})$ (for some basis). Let $S_M \subset \mathbb{Z}$ denote the set of all integers that are not multiples of p^2 for any prime $p \leq M$. Then

$$\lim_{N\to\infty} \frac{\#\{x \in V(\mathbb{Z}) \cap B_N : f(x) \in S_M\}}{(2N+1)^m} = \prod_{p \leq M} (1 - c_p/p^{2m})$$

by the Chinese Remainder Theorem, since we are only imposing congruence conditions at finitely many primes. Letting M go to infinity, and using the exercise on doubly-indexed sequences, we have that

$$\limsup_{N\to\infty} \frac{\#\{x \in V(\mathbb{Z}) \cap B_N : f(x) \text{ squarefree}\}}{(2N+1)^m} \le \prod_p (1 - c_p/p^{2m}).$$

(This upper bound indeed holds for any polynomial.)

For the lower bound, as we did earlier, we will use a tail estimate.

First observe that by Condition 1, the non-generic points in B_N have vanishing density as $N \to \infty$, so we may ignore them.

Let $W_p \subset V(\mathbb{Z})$ denote the set of points v with $p^2 | f(v)$. For the generic points in $B_N \cap W_p^{\text{gen}}$, i.e. the generic points in B_N where f is a multiple of p^2, we will cover a large portion of B_N by fundamental domains for the action of $G(\mathbb{Z})$ on $V(\mathbb{R})$ and then use the density formula we proved in the fundamental domain.

Observe that B_N is covered by a countable union $\cup_{i=1}^{\infty} \gamma_i \mathcal{F}_X$ of translates of $\mathcal{F}_X$ (taken over $\gamma_i \in G(\mathbb{Z})$) where X is sufficiently large so that $|I(v)| < X$ for all $v \in B_N$. Since I has degree d, we may take $X = cN^d$ for some fixed constant $c > 0$.

Let $B_{N,s} := B_N \cap \cup_{i=1}^{s} \gamma_i \mathcal{F}_X$. By the tail estimate applied once for each fundamental domain $\gamma_i \mathcal{F}$, we have that

$$\begin{aligned}\left| B_{N,s} \cap \bigcup_{p>M} W_p^{\text{gen}} \right| &= sO_\varepsilon(X^{m/d}/(M^{\min(\eta,1)} \log M) + X^{\frac{m-1}{d}}) + sO(\varepsilon X^{m/d}) + so(X^{m/d}) \\ &= sO_\varepsilon(N^m/(M^{\min(\eta,1)} \log M) + N^{m-1}) + sO(\varepsilon N^m) + so(N^m).\end{aligned}$$

Let $S_p = \{v \in V(\mathbb{Z}) : p^2 \nmid f(v)\}$ and $S = \cap_p S_p$. Observe that (as we used before)

$$\bigcap_{p \le M} S_p \subset \left(S \cup \bigcup_{p>M} W_p \right)$$

and thus

$$\left| B_{N,s} \cap \bigcap_{p \le M} S_p^{\text{gen}} \right| \le |B_{N,s} \cap S^{\text{gen}}| + \left| B_{N,s} \cap \bigcup_{p>M} W_p^{\text{gen}} \right|.$$

Thus

$$\liminf_{N\to\infty}\frac{\#\{x\in V(\mathbb{Z})\cap B_{N,s}:f(x)\text{ squarefree}\}}{\mathrm{vol}(B_{N,s})}$$
$$\geq\prod_{p\leq M}(1-c_p/p^{2m})+sO_\varepsilon(1/(M^{\min(\eta,1)}\log M))+sO(\varepsilon).$$

Let $M\to\infty$, then $\varepsilon\to 0$, and then $s\to\infty$ to obtain the desired lower bound:

$$\liminf_{N\to\infty}\frac{\#\{x\in V(\mathbb{Z})\cap B_N:f(x)\text{ squarefree}\}}{\mathrm{vol}(B_N)}\geq\prod_p(1-c_p/p^{2m}).$$

This completes the proof of Theorem 4.2.

4.4 Verifying the hypotheses for f_3, f_4, f_5

Let $n\in\{3,4,5\}$. For any ring T, let $V(T)$ denote

1. the space $\mathrm{Sym}_3 T^2$ of binary cubic forms with coefficients in T if $n=3$,
2. the space $T^2\otimes_T \mathrm{Sym}_2 T^3$ of pairs of ternary quadratic forms with coefficients in T if $n=4$, or
3. the space $T^4\otimes_T \wedge^2 T^5$ of quadruples of 5×5 skew-symmetric matrices with entries in T if $n=5$.

For these three cases, respectively, the associated algebraic group G acting on V is

1. $\mathbf{GL}_2$ for the natural action tensored with $\det^{-1}$,
2. $\mathbf{GL}_2\times\mathbf{SL}_3$ for the natural action, or
3. $\mathbf{GL}_4\times\mathbf{SL}_5$ for the natural action.

It is a non-trivial fact that these are all *prehomogeneous spaces*, i.e. each representation V possesses a Zariski-open orbit of G.

We will call an orbit of $G(T)$ on $V(T)$ nondegenerate if the discriminant (i.e. value of f) of any element in that orbit is nonzero.

The nondegenerate orbits of $G(T)$ on $V(T)$ for a field T shown by Wright–Yukie [WY92] to be canonically in bijection with isomorphism classes of étale T-algebras of rank $n \in \{3,4,5\}$, resp.

The nondegenerate orbits of $G(\mathbb{Z})$ on $V(\mathbb{Z})$ were classified by Bhargava:

Theorem 4.6. *The nondegenerate orbits of $G(\mathbb{Z})$ on $V(\mathbb{Z})$ are canonically in bijection with isomorphism classes of pairs (R, R') where R is a commutative ring with unit which is a free $\mathbb{Z}$-module of rank n and R' is a resolvent ring of R. In this bijection, the discriminant of an element $v \in V(\mathbb{Z})$ equals the discriminant of the corresponding ring R. Furthermore, every such ring R arises as (R, R') at least once in this bijection, and if R is maximal then it occurs exactly once.*

A resolvent ring of a (cubic, quartic, or quintic) ring R is a (quadratic, cubic, or sextic) ring R' that satisfies certain properties, e.g. R' has the same discriminant as R.

4.4.1 Remark: Integral orbits on closed orbits

Note the importance of having an *open* orbit in V. For the *closed* orbits, there is the fundamental and general theorem of Borel–Harish-Chandra.

Theorem 4.7 (Borel–Harish-Chandra 1962)**.** *Let G be a reductive group defined over $\mathbb{Z}$, $\pi\colon G \to \mathbf{GL}(V)$ a rational $\mathbb{Q}$-representation, Γ a $G(\mathbb{Z})$-stable lattice in $V(\mathbb{Q})$, and $O \subset V$ a* closed *orbit of G. Then $O \cap \Gamma$ consists of a finite number of orbits of $G(\mathbb{Z})$.*

The open orbit $\{f \neq 0\} \subset V$ of a prehomogeneous space may be identified with a *closed* orbit in a *larger* representation: for any integer d, there is the canonical isomorphism

$$\{f \neq 0\} \cong O_d = \{(v,t) : f(v)t = d\} \subset V \times \mathbb{A}^1_{\chi^{-1}}$$

where $\chi\colon G \to \mathbb{G}_m$ is the character for which $f\colon V \to \mathbb{A}^1$ is χ-equivariant.

The theorem of Borel–Harish-Chandra says that

$$G(\mathbb{Z})\backslash O_d(\mathbb{Z}) = \{(v,t) \in \mathbb{Z}^2 : f(v)t = d\}$$

is finite. The larger affine space $V \times \mathbb{A}^1_{\chi^{-1}}$ “sees” the values of f, and the integrality hypothesis now enforces the strong restriction that $f(v)$ divides d.

In particular, unbounded ramification can only occur in an *open* orbit.

4.4.2 Where do these orbit parametrizations come from?

Reference: [Bha08].

To verify the six conditions, we will need to know more about how the points of these orbit parametrizations correspond to rings.

There is a natural mapping which associates to any nondegenerate ring R of rank n and basis $\overline{\alpha}$ of $R/\mathbb{Z}$ a set $X_{R,\overline{\alpha}}(\mathbb{C})$ of n points in $\mathbb{P}^{n-2}(\mathbb{C})$. First, following [Bha08], we give an explicit construction with coordinates. Then we give a coordinate-free construction.

Fix a $\mathbb{Z}$-basis $\alpha = \langle \alpha_0 = 1, \alpha_1, \ldots, \alpha_{n-1}\rangle$ of R. Since R is nondegenerate, $K = R \otimes \mathbb{Q}$ is an étale $\mathbb{Q}$-algebra of dimension n, and there are n distinct $\mathbb{Q}$-algebra homomorphisms $\rho^{(1)}, \ldots, \rho^{(n)}$ from K to $\mathbb{C}$. For any $\alpha \in K$, let $\alpha^{(k)} = \rho^{(k)}(\alpha) \in \mathbb{C}$. Let $\langle \alpha_0^*, \ldots, \alpha_{n-1}^*\rangle$ be the dual basis under the trace pairing. For $k \in \{1, \ldots, n\}$ set

$$x_R^{(k)} = [\alpha_1^{*(k)} : \cdots : \alpha_{n-1}^{*(k)}] \in \mathbb{P}^{n-2}(\mathbb{C}).$$

We have constructed a set $X_{R,\alpha}(\mathbb{C}) = \{x_R^{(1)}, \ldots, x_R^{(n)}\} \subset \mathbb{P}^{n-2}(\mathbb{C})$ depending only on the ring R and the latter $n-1$ elements of the basis $\langle \alpha_0, \ldots, \alpha_{n-1}\rangle$.

Exercise: Show that $X_{R,\alpha}(\mathbb{C})$ only depends on R and the $\mathbb{Z}$-basis $\overline{\alpha} = \langle \overline{\alpha}_1, \ldots, \overline{\alpha}_{n-1}\rangle$ of $R/\mathbb{Z}$.

In fact, the set $X_{R,\overline{\alpha}}(\mathbb{C})$ arises naturally as the set of $\mathbb{C}$-points of the image of $\operatorname{Spec} R$ under a certain rational map $\phi_{\overline{\alpha}}\colon \operatorname{Spec} R \dashrightarrow \mathbb{P}^{n-2}_{\mathbb{Z}}$ constructed using $\overline{\alpha}$.

Indeed, recall the *inverse different* $\mathcal{D}^{-1}$ is the R-submodule of K equal to $\{a \in K : \operatorname{tr}^K_{\mathbb{Q}}(ax) \in \mathbb{Z}$ for all $x \in R\}$. We have already defined a $\mathbb{Z}$-basis of $\mathcal{D}^{-1}$,

$$\alpha = \langle \alpha_0^*, \ldots, \alpha_{n-1}^*\rangle \subset \mathcal{D}^{-1}.$$

Suppose for simplicity that R is *Gorenstein*, i.e. the inverse different is *invertible* as an R-module. Then we have a basis α of global sections of a line bundle $\mathcal{D}^{-1}$ on $\operatorname{Spec} R$ with no base locus. This determines a *morphism* to projective space over $\mathbb{Z}$:

$$\begin{aligned}\phi_\alpha\colon \operatorname{Spec} R &\to \mathbb{P}^{n-1}_{\mathbb{Z}}\\ x &\mapsto [\alpha_0^*(x) : \cdots : \alpha_{n-1}^*(x)].\end{aligned}$$

Since $\alpha_1^*, \dots, \alpha_{n-1}^*$ all vanish on 1, the point $[\alpha_1^*(x) : \cdots : \alpha_{n-1}^*(x)]$ lies in a fixed hyperplane $\mathbb{P}^{n-2}_{\mathbb{Z}} \subset \mathbb{P}^{n-1}_{\mathbb{Z}}$, and we obtain a morphism

$$\begin{aligned}\phi_{\overline{\alpha}}\colon \operatorname{Spec} R &\to \mathbb{P}^{n-2}_{\mathbb{Z}}\\ x &\mapsto [\alpha_1^*(x) : \cdots : \alpha_{n-1}^*(x)].\end{aligned}$$

It is easy to check that this morphism is a closed immersion. The finite set $X_{R,\overline{\alpha}}(\mathbb{C})$ is recovered as the set of $\mathbb{C}$-points of the image of $\phi_{\overline{\alpha}}$.

For small values of n, it is possible to find a space V of homogeneous tensor functions on $\mathbb{A}^n_{\mathbb{Z}}$ such that for each $(R, \overline{\alpha})$ there is a tensor $x \in V$ whose "degeneracy locus" X_x in $\mathbb{P}^{n-2}_{\mathbb{Z}}$ is birational to $\operatorname{im}(\phi_{R,\overline{\alpha}}) \subset \mathbb{P}^{n-2}_{\mathbb{Z}}$. (If R is Gorenstein, then birational can be upgraded to isomorphic.)

In each case, there is a natural symmetry group G acting on V with the property that x and gx are associated with the same ring R whenever $g \in G(\mathbb{Z})$. In favorable cases, the space V has a Zariski-open orbit.

If $n = 3$, then $x \in V$ is a nondegenerate binary cubic, and X_x is defined to be the 3 roots of x in $\mathbb{P}^{3-2}$.

If $n = 4$, then x determines a pair of conics in $\mathbb{P}^{4-2}$, and X_x is defined to be the intersection of these two conics (this will generally have 4 points).

If $n = 5$, then x gives us four 5×5 skew-symmetric matrices. Regarding the first tensor factor $\mathbb{A}^4$ in V as the space of linear forms on a four-dimensional affine space, we may equivalently regard x as a single 5×5 skew-symmetric matrix M whose entries are linear forms. To construct functions which cut out $X_x \subset \mathbb{P}^{5-2} = \mathbb{P}^{4-1}$ we will use the principal 4×4 minors of M.

Exercise: Let A be an $n \times n$ skew-symmetric matrix. If n is odd, then $\det A = 0$. If n is even, then there is a polynomial pfa of degree $n/2$ in the $\binom{n}{2}$ independent entries of A (which is independent of A) such that $\det A = \operatorname{pfa}(A)^2$. The quantity $\operatorname{pfa}(A)$ (which is a canonically determined square-root of the determinant up to sign) is called the Pfaffian of A.

The determinants of the five principal 4×4 minors of M are degree four squares of Pfaffians in four variables. For generic x, these five Pfaffians will be linearly independent. These Pfaffians cut out *quadrics* in $\mathbb{P}^3_{\mathbb{Z}}$ which will generically intersect in 5 points.

In fact, for a generic set X of five points in $\mathbb{P}^3_{\mathbb{C}}$, the family of quadratic forms F_X which vanish at X is five dimensional (the space of all quadratic forms on $\mathbb{P}^3_{\mathbb{C}}$ is 10 and vanishing at a point is a linear condition). When x is generic, its associated five Pfaffians will span F_X.

4.4.3 Verifying the six conditions

Now we verify that the six conditions are satisfied for f_3, f_4, f_5. As we will see, the first five conditions essentially follow from arguments which apply uniformly for prehomogeneous spaces whose open orbits have finite stabilizers. For the sixth condition we will use ad hoc arguments.

Recall that we need a notion of "generic". We call any nondegenerate orbit of $V(\mathbb{Z})$ generic if it corresponds to an order in a degree n number field with Galois group S_n.

A direct calculation shows that the open orbit of V is isomorphic to G/S_n for $n = 3, 4, 5$. Note this only needs to be verified on a single element in the open orbit. E.g. the stabilizer of the binary cubic form

$$(x + y)(x^2 + xy + y^2)$$

in $\mathbf{GL}_2(\mathbb{C})$ is a copy of S_3 generated by $(x, y) \mapsto (y, x)$ and $(x, y) \mapsto (\zeta x, \zeta y)$ where ζ is a primitive 3rd root of unity. Explicitly, it is the group

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \zeta & 0 \\ 0 & \zeta \end{pmatrix}, \begin{pmatrix} 0 & \zeta \\ \zeta & 0 \end{pmatrix}, \begin{pmatrix} \zeta^2 & 0 \\ 0 & \zeta^2 \end{pmatrix}, \begin{pmatrix} 0 & \zeta^2 \\ \zeta^2 & 0 \end{pmatrix}.$$

This shows Condition 2.

Consider the S_n-torsor

$$\pi \colon G \to G/S_n.$$

The fiber of π over any point of G/S_n is a S_n-torsor over that point; in particular, the fiber of π over any rational point is $\operatorname{Spec} \widehat{K}$ where $\widehat{K}$ is an étale $\mathbb{Q}$-algebra equipped with an action of S_n. The subset of integral points in $(G/S_n)(\mathbb{Q})$ for which the $\mathbb{Q}$-algebra $\widehat{K}^{S_{n-1}}$ is not a field with Galois group S_n is a thin set.

By S. Cohen's estimate on thin sets (Theorem 3.2), such points form a vanishing proportion among all integral points. This proves Condition 1.

We will take $I = f_n$ for Condition 3 (homogeneous G_1-invariant). Since f_n is equivariant for the determinant character of V, it is G_1-invariant.

Condition 4 (existence of fundamental domains homogeneously expanding w.r.t. I) essentially follows from the existence of Siegel sets for $G(\mathbb{Z})$ acting on $G(\mathbb{R})$ since the open orbit of V can be identified with G up to a finite stabilizer. There is a small complication since the real points of the open orbit break up into several $G(\mathbb{R})$-orbits over $\mathbb{R}$ (depending on the number of real roots), and each real component may have a different stabilizer.

Condition 5 (CRT in the fundamental domain) essentially follows from usual CRT since V is just affine space, but there is a complication due to the cusps (noncompactness of $\mathcal{F}_X$). One must compactly approximate $\mathcal{F}_X$ to apply CRT, and then verify that the number of lattice points in the set defined by finitely many congruences which lie in the cusps is vanishingly small.

We now verify Condition 6 for f_3, f_4, f_5 with parameters

$$a = 2, \qquad c = \binom{n}{2}, \qquad k = 0.$$

Then Conditions 6(ii) and 6(iv) are automatically satisfied.

Now we verify Conditions 6(1) and 6(iii). A nondegenerate element of $\overline{x} \in V(\mathbb{F}_p)$ determines n distinct points $X_{\overline{x}}$ in $\mathbb{P}^{n-2}_{\mathbb{F}_p}(\overline{\mathbb{F}}_p)$.

Recall that each $x \in V$ has a "degeneracy locus" $X_x \subset \mathbb{P}^{n-2}_{\mathbb{Z}}$ which is birational to $\operatorname{Spec} R$ and if R is Gorenstein then X_x is isomorphic to $\operatorname{Spec} R$.

We claim that for any (large) prime p, the discriminant $f(\overline{x}) \in \mathbb{F}_p$ of an element $\overline{x} \in V(\mathbb{F}_p)$ vanishes if and only if either $X_{\overline{x}} \subset \mathbb{P}^{n-2}_{\mathbb{F}_p}$ is finite and has fewer than n points or $\dim X_{\overline{x}} > 0$.

In general, if the rational map $\operatorname{Spec} R \dashrightarrow \mathbb{P}^{n-2}_{\mathbb{Z}}$ is defined at p then $X_{\overline{x}} \cong \operatorname{Spec} R \otimes \mathbb{F}_p$ and thus $X_{\overline{x}}$ will have fewer than n points if R is ramified at p.

It is possible for $\dim X_{\overline{x}} > 0$ — e.g. f may have all its coefficients divisible by p.[4] For such p the ring R cannot be Gorenstein, thus R must also be ramified at p (since unramified implies

[4] [Is Deligne's argument in his letter to GGS for cubic rings, that the morphism extends over the non-Gorenstein locus, really correct?]

Gorenstein). So in either case, the discriminant $f(\overline{x})$ will vanish.

The latter case where a subvariety $X_{\overline{x}}$ of $\mathbb{P}^{n-2}_{\mathbb{F}_p}$ of positive dimension is cut out by $\overline{x} \in V(\mathbb{F}_p)$ occurs on a subvariety of $V_{\mathbb{F}_p}$ of positive codimension. Indeed for $n = 3$ this does not occur (except for very few cases when $\overline{x} \equiv 0 \pmod{p}$). When $n = 4, 5$ this can only happen when multiple forms cut out the same subvariety of $V_{\mathbb{F}_p}$ which can only happen if the coefficients reduce mod p to a subvariety of V of positive codimension.

Similarly, the case where strictly fewer than $n-1$ points are cut out by $\overline{x} \in V(\mathbb{F}_p)$ also occurs on a subvariety of positive codimension. These two cases correspond to strong multiples of p^2, i.e. the image of $W_p^{(1)}$ in $V(\mathbb{F}_p)$.

The image of $W_p^{(2)}$ in $V(\mathbb{F}_p)$ consists of the remaining case, which is when exactly $n-1$ points are cut out by $\overline{x} \in V(\mathbb{F}_p)$.

We now determine the points of $V(\mathbb{Z}/p^2\mathbb{Z})$ whose discriminant is *weakly* a multiple of p^2. Let $x(s,t) \in V(\mathbb{Z})$ have discriminant weakly a multiple of p^2. The reduction $\overline{x} \pmod{p}$ of x has a double (but not triple) root in $\mathbb{P}^1$. This implies that $\overline{x}$ is $G^1(\mathbb{F}_p)$-equivalent to

$$\overline{a}s^3 + \overline{b}s^2t$$

where $\overline{a}, \overline{b} \in \mathbb{F}_p$ and $\overline{b} \neq 0$. It's well-known that $G^1(\mathbb{Z}) \to G^1(\mathbb{Z}/p\mathbb{Z})$ is surjective, so $x(s,t)$ is $G(\mathbb{Z})$-equivalent to a binary cubic form of the form $as^3 + bs^2t + cst^2 + dt^3$ where b is coprime to p and c, d are multiples of p. The discriminant $f_3(x)$ satisfies

$$f_3(x) \equiv -4b^3d \pmod{p^2}$$

and thus (for $p > 2$) d must be a multiple of p^2. Observe that

$$x' = \begin{pmatrix} 1 & \\ & 1/p \end{pmatrix} (as^3 + bs^2t + cst^2 + dt^3) = pas^3 + bs^2t + (c/p)st^2 + (d/p^2)t^3 \in V(\mathbb{Z})$$

and that its discriminant is equal to $\pm f_3(x)/p^2$.

Such an x corresponds to a ring R which is not maximal at p (i.e. $R \otimes \mathbb{Z}_p$ is not maximal in $R \otimes \mathbb{Q}_p$), and x' corresponds to an overring $R' \supset R$ in which R is index p. $x' \not\equiv 0 \pmod{p}$. A cubic ring R' has at most 3 subrings of index p. More precisely:

Lemma 4.8. *The number of index p subrings of $R = R_x$ is equal to the number of roots of $x \pmod{p}$ in $\mathbb{P}^1(\mathbb{F}_p)$.*

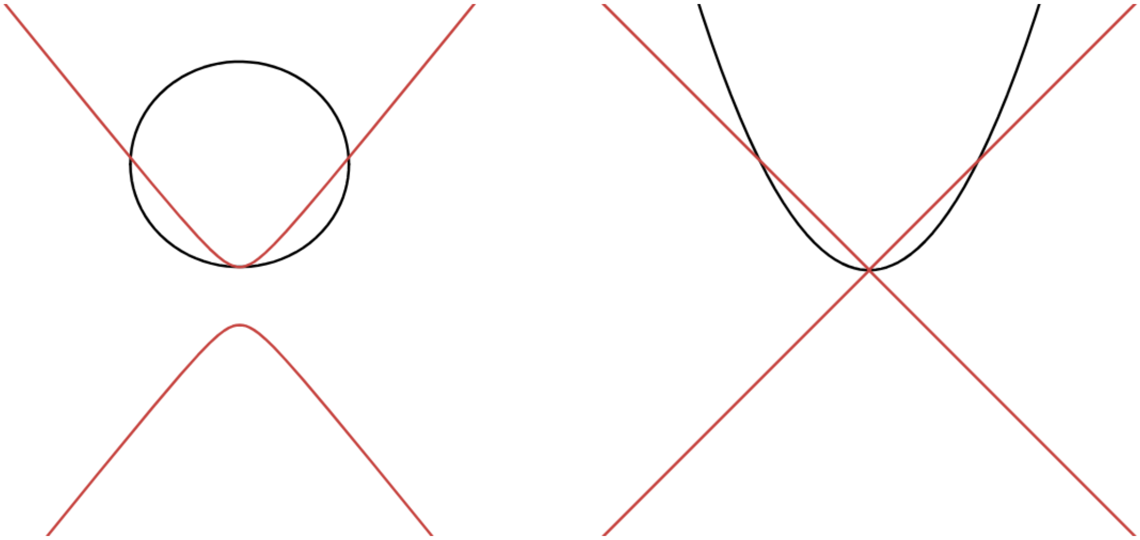

Figure 2: Degenerating a pair of conics.

This shows Condition 6(iii).

Now suppose $n = 4$. The image of $W_p^{(2)}$ in $V(\mathbb{F}_p)$ consists of pairs $(\overline{A}, \overline{B})$ of ternary quadratic forms with precisely three common zeros in $\mathbb{P}^2(\overline{\mathbb{F}}_p)$. The unique double zero will be $\mathbb{F}_p$-rational so it may be sent to $[1:0:0]$ by an element of $\mathbf{SL}_3(\mathbb{F}_p)$. The action of $\mathbf{SL}_2(\mathbb{F}_p)$ on $V(\mathbb{F}_p)$ takes a pair of ternary quadratic forms $\overline{x} = \overline{A}s + \overline{B}t$ to another pair $x' = \overline{A}'s + \overline{B}'t$ whose coefficients are linear combinations of $\overline{A}$ and $\overline{B}$.

By degenerating this pair via $\mathbf{SL}_2(\mathbb{F}_p)$, we can ensure that $\overline{A}'$ cuts out a pair of lines intersecting at $[1:0:0]$ and $\overline{B}'$ cuts out a nonsingular conic passing through $[1:0:0]$ which is not tangent to either of these lines. In terms of the associated pair of symmetric matrices, the pair x' takes the form

$$\left(\begin{bmatrix} \overline{a}_{11} & \overline{a}_{12} & \overline{a}_{13} \\ \overline{a}_{12} & \overline{a}_{22} & \overline{a}_{23} \\ \overline{a}_{13} & \overline{a}_{23} & \overline{a}_{33} \end{bmatrix}, \begin{bmatrix} \overline{b}_{11} & \overline{b}_{12} & \overline{b}_{13} \\ \overline{b}_{12} & \overline{b}_{22} & \overline{b}_{23} \\ \overline{b}_{13} & \overline{b}_{23} & \overline{b}_{33} \end{bmatrix} \right)$$

where $\overline{a}_{11} = \overline{b}_{11} = \overline{b}_{12} = \overline{b}_{13} = 0$ and $\overline{b}_{22}\overline{b}_{33} - \overline{b}_{23}^2 \neq 0$. These divisibility constraints on x' imply that its discriminant satisfies

$$f_4(x') := \mathrm{Disc}(\det(A's + B't)) \equiv b_{11}(b_{22}b_{33} - b_{23}^2)C^3 \pmod{p^2}$$

where C is the coefficient of s^2t in $\det(A's + B't)$. From this, we see that if C were divisible by p then $f_4(x')$ would be *strongly* a multiple of p^2. Thus for $f_4(x')$ to be *weakly* a multiple of p^2 it must be that b_{11} is divisible by not only p but also p^2.

So, if $f_4(x) = f_4(x')$ is weakly divisible by p^2, then x' satisfies the above divisibility constraints, namely $\overline{a}_{11} = \overline{b}_{12} = \overline{b}_{13} = 0$, $\overline{b}_{22}\overline{b}_{33} - \overline{b}_{23}^2 \neq 0$, $C \not\equiv 0 \pmod{p}$, and $b_{11} \equiv 0 \pmod{p^2}$. Thus we may multiply A by p and then divide the entries of the first row and column of both A and B by p and obtain a new integral form x''. This corresponds to applying the transformation

$$g = \left(\begin{bmatrix} 1/p & \\ & 1 \end{bmatrix}, \begin{bmatrix} 1/p & & \\ & 1 & \\ & & 1 \end{bmatrix} \right) \in G(\mathbb{Q}).$$

Thus $f_4(x'') = f_4(x')/p^2 = f_4(x)/p^2$, which verifies Condition 6(i) with $a = 2$.

For $n = 5$ there are more complicated but analogous arguments. See [Bha14].

This completes our proof for the expected density of squarefree values for the discriminant polynomials f_3, f_4, f_5.

4.5 The density of S_n-number fields with squarefree discriminant

The density of squarefree values for the discriminant polynomials f_3, f_4, f_5 may be regarded as a statement about the density of rank n rings with squarefree density.

Orders with squarefree discriminant are necessarily maximal, and thus in one-to-one correspondence with $\mathbb{Q}$-algebras with Galois group S_n. The *generic* points with squarefree discriminant, which have 100% density, are in one-to-one correspondence with S_n-fields. *Computing the density* of squarefree values for these polynomials now proves the following theorem:

Theorem 4.9. *Let $n = 3, 4$ or 5 and let $N_n^{\mathrm{sqf}}(X)$ denote the number of isomorphism classes of number fields of degree n that have squarefree discriminant of absolute value less than X. Then*

$$N_n^{\mathrm{sqf}}(X) = \frac{r_2(S_n)}{3 \cdot n!}\zeta(2)^{-1} \cdot X + o(X)$$

where $r_2(S_n)$ denotes the number of 2-torsion elements in the symmetric group S_n.

In fact one can work more generally (by Condition 5) and compute the density of number fields satisfying *arbitrary local conditions* for primes in some *finite* set S, and which have p-squarefree discriminant for $p \notin S$.

More precisely, let $\Sigma = (\Sigma_v)_v$ denote a set of local specifications for degree n number fields, i.e. Σ_v is a set of degree n étale $\mathbb{Q}_v$-algebras.

We assume that for sufficiently large primes p the set Σ_p contains all unramified and simply ramified étale degree n extensions of $\mathbb{Q}_p$. Also assume that Σ_∞ contains all the étale extensions of $\mathbb{R}$ of degree n.

Let $S_p = S_p(\Sigma_p)$ denote the subset of points of $V(\mathbb{Z})$ corresponding to rings R such that $R \otimes \mathbb{Z}_p$ is the *ring of integers* of some étale extension in Σ_p.

The generic elements of $S = \cap_p S_p$ are the rings of integers in S_n-fields that agree with the local specifications of Σ.

First we compute

$$\mu_p(\{x \in V(\mathbb{Z}_p) : R_x[\tfrac{1}{p}] \in \Sigma_p, R_x \text{ maximal}\}).$$

Choose an additive Haar measure dx on $V(\mathbb{Q}_p)$ and a Haar measure dg on $G(\mathbb{Q}_p)$. Normalize these measures so that $dx(V(\mathbb{Z}_p)) = 1$ and $dg(G(\mathbb{Z}_p)) = \#G(\mathbb{F}_p)p^{-\dim G}$. (This latter choice of "local convergence factor" is made to ensure that we get a convergent measure on the adelic group $G(A)$ from the product of these local measures.)

The additive Haar measure dx on $V(\mathbb{Q}_p)$ transforms like $dx \mapsto g_*(dx) = |\det g|_p \, dx$ under g, which means $|f(x)|_p^{-1}dx$ is $G(\mathbb{Q}_p)$-invariant (since $|f(gx)|_p^{-1}g_*(dx) = |f(x)|_p^{-1}dx$).

Thus for any $x \in V(\mathbb{Z}_p)$, the Haar measure dg pushes forward under $\pi\colon G(\mathbb{Z}_p) \to G(\mathbb{Z}_p) \cdot x : g \mapsto gx$ to $c \cdot |f(x)|_p^{-1}dx$ for some positive constant $c = c_x$ (only depending on the orbit $G(\mathbb{Z}_p)x$). A direct calculation shows that $c_R = |G_x|$ where G_x is the stabilizer subgroup of x in $G(\mathbb{Z}_p)$.. So $\int_A dx = |G_x|^{-1} \int_{\pi^{-1}A} |f(\pi g)|_p dg$ for any measurable subset $A \subset G(\mathbb{Z}_p) \cdot x$.

Fix a *maximal* $\mathbb{Z}_p$-algebra R arising as (R, R') corresponding to some $x \in V(\mathbb{Z}_p)$. Since R is maximal, it arises as (R, R') for a unique resolvent ring R'. If $y \in V(\mathbb{Z}_p)$ is also associated with R, then it necessarily corresponds to (R, R'), and thus is in the $G(\mathbb{Z}_p)$-orbit of x. Then

$$\begin{aligned}\mu_p(\{y \in V(\mathbb{Z}_p) : R_y \cong R\}) = \mu_p(G(\mathbb{Z}_p)\cdot x) &= \int_{x\in G(\mathbb{Z}_p)\cdot x} dx \\ &= \frac{1}{|G_x|}\int_{g\in G(\mathbb{Z}_p)} |f(gx)|_p\, dg \\ &= \frac{|G(\mathbb{F}_p)|p^{-\dim G}}{|G_x|}|f(x)|_p. \\ &= |G(\mathbb{F}_p)|p^{-\dim G}\cdot\frac{|\mathrm{Disc}(R)|_p}{|\mathrm{Aut}(R)|}.\end{aligned}$$

Thus

$$\mu_p(\{x \in V(\mathbb{Z}_p) : R_x[\tfrac{1}{p}] \in \Sigma_p, R_x \text{ maximal}\}) = |G(\mathbb{F}_p)|p^{-\dim G}\cdot\sum_{K\in\Sigma_p}\frac{|\mathrm{Disc}(R_K)|_p}{|\mathrm{Aut}(R_K)|}.$$

We have not yet used any properties of Σ. To evaluate the sums on the right-hand side, we will use a "mass formula" for local extensions.

Theorem 4.10 (Serre–Bhargava mass formula [Ser78], [Bha07]). *For any splitting type λ of degree n,*

$$\sum_{K/\mathbb{Q}_p\,:\,\mathrm{spl}(K,p)=\lambda} |\mathrm{Disc}(K)|_p\cdot|\mathrm{Aut}(K)|^{-1} = \left(\prod_{f^e\in\lambda}\frac{1}{p^{f(e-1)}}\cdot\frac{1}{f}\right)\cdot\frac{1}{|\mathrm{Aut}(\lambda)|}.$$

Here $|\mathrm{Aut}(\lambda)|$ is defined to be the number of permutations of the factors $f_i^{e_i}$ of λ which preserve λ.

The $\mathbb{Q}_p$-algebra K has squarefree discriminant if and only if either p is unramified, or $p > 2$ and the splitting type $\mathrm{spl}(K,p)$ of p in K is of the form $\lambda = (f_1^2 f_2^1 \cdots f_r^1)$. In particular, the local condition that $K \in \Sigma_p$ is determined by splitting conditions for all but finitely many p.

Summing the mass formula over these two possible splitting types consistent with squarefree discriminant obtains

$$\sum_{R \text{ sqf}}\frac{|\mathrm{Disc}(R)|_p}{|\mathrm{Aut}(R)|} = \begin{cases}1+1/p & \text{if } p>2\\ 1 & \text{if } p=2.\end{cases}$$

Our earlier work has shown (1):

$$\lim_{X\to\infty} \frac{|\mathcal{F}_X \cap S^{\text{gen}}|}{X^{m/d}\text{Vol}(\mathcal{F}_1)} = \prod_p \mu_p(S)$$

where $\mu_p(S)$ is the density of the topological closure of S in $V(\mathbb{Z}_p)$. Recall that $\mu_p(S)$ denotes the measure of the p-adic closure $S^p \subset V(\mathbb{Z}_p)$ of S.

We claim that

$$S^p = \{x \in V(\mathbb{Z}_p) : R_x[\tfrac{1}{p}] \in \Sigma_p, R_x \text{ maximal}\}.$$

The containment $\subset$ is clear. What is unclear is why we should be able to p-adically approximate to arbitrary precision any $x \in V(\mathbb{Z}_p)$ on the right-hand side by an *integral* $x' \in V(\mathbb{Z})$ whose associated *global* ring R has square-free discriminant.

Assume the claim. Then

$$\begin{aligned}\lim_{X\to\infty} \frac{|\mathcal{F}_X \cap S^{\text{gen}}|}{X^{m/d}\text{Vol}(\mathcal{F}_1)} &= |G(\mathbb{F}_2)|2^{-\dim G}\prod_{p>2}|G(\mathbb{F}_p)|p^{-\dim G}(1+1/p)\\ &= \frac{2}{3}\prod_p |G(\mathbb{F}_p)|p^{-\dim G}(1+1/p)\end{aligned}$$

and so

$$|\mathcal{F}_X \cap S^{\text{gen}}| = X\text{Vol}(\mathcal{F}_1)\frac{2}{3}\prod_p |G(\mathbb{F}_p)|p^{-\dim G}(1+1/p) + o(X).$$

Now we evaluate the leading constant. The fundamental domain $\mathcal{F} \subset V^{\text{op}}(\mathbb{R})$ for $G(\mathbb{Z})$ is the union over connected components of $V^{\text{op}}(\mathbb{R})$ of the image of a fundamental domain of $G(\mathbb{R})$ for the action of $G(\mathbb{Z})$. Let n_i be the order of the stabilizer subgroup of any point in the ith connected component of $V^{\text{op}}(\mathbb{R})$. Then

$$\text{vol}(\mathcal{F}_1) = [G(\mathbb{Z}) : G^1(\mathbb{Z})]\text{vol}(G^1(\mathbb{R})/G^1(\mathbb{Z}))\sum_{i=1}^{t}\frac{1}{n_i}.$$

The connected components of $V^{\text{op}}(\mathbb{R})$ are in bijection with the set Σ_∞ of isomorphism classes of rank n étale $\mathbb{R}$-algebras, and n_i is the order of the automorphism group of the ith isomorphism class. Thus

$$\text{vol}(\mathcal{F}_1) = \frac{1}{2}\text{vol}(G_1(\mathbb{R})/G_1(\mathbb{Z}))\sum_{K\in\Sigma_\infty}\frac{1}{\#\text{Aut}(K)}.$$

Thus the leading constant is

$$\left(\frac{1}{2}\mathrm{vol}(G_1(\mathbb{R})/G_1(\mathbb{Z}))\sum_{K\in\Sigma_\infty}\frac{1}{\#\mathrm{Aut}(K)}\right)\frac{2}{3}\prod_p |G(\mathbb{F}_p)|p^{-\dim G}(1+1/p)$$

We claim that

$$\sum_{K\in\Sigma_\infty}\frac{1}{\#\mathrm{Aut}(K)}=\frac{r_2(S_n)}{n!}.$$

Indeed, the set Σ_∞ of all isomorphism classes of étale degree n $\mathbb{R}$-algebras is in bijection with the set of non-isomorphic ways that $\pi_1(\mathbb{R})=\mathbb{Z}/2\mathbb{Z}$ can act on n elements, i.e. the homomorphisms $\varphi\colon\mathbb{Z}/2\mathbb{Z}\to S_n$ up to S_n-conjugacy. Since $\#\mathrm{Aut}(K_\varphi)=\#Z(\varphi)$ where $Z(\varphi)\subset S_n$ is the stabilizer of φ, by the orbit-stabilizer theorem ("groupoid cardinality") we have that

$$\sum_{K\in\Sigma_\infty}\frac{1}{\#\mathrm{Aut}(K)}=\frac{|\{\varphi\colon\mathbb{Z}/2\mathbb{Z}\to S_n\}|}{|S_n|}=\frac{r_2(S_n)}{n!}.$$

The Tamagawa number of a product of special/general linear groups is 1:

$$\tau(G_1)=\mathrm{vol}(G_1(\mathbb{R})/G_1(\mathbb{Z}))\prod_p |G^1(\mathbb{F}_p)|p^{-\dim G^1}=1.$$

Note that $|G(\mathbb{F}_p)|p^{-\dim G}=|G^1(\mathbb{F}_p)|p^{-\dim G^1}(1-1/p)$.

Putting this all together, the leading constant is

$$\left(\frac{1}{2}\mathrm{vol}(G_1(\mathbb{R})/G_1(\mathbb{Z}))\sum_{K\in\Sigma_\infty}\frac{1}{\#\mathrm{Aut}(K)}\right)\frac{2}{3}\prod_p |G(\mathbb{F}_p)|p^{-\dim G}(1+1/p)=\frac{r_2(S_n)}{3\cdot n!}\zeta(2)^{-1}.$$

5 Monic cubic abelian polynomials

We now return to discuss some more recent results on the subject of random polynomials, joint with Shubhrajit Bhattacharya [BO23].

Let F denote the set of polynomials of the form $t^3-t^2+at+b\in\mathbb{Z}[t]$ which have Galois group C_3, the cyclic group of order three.

Theorem 5.1. *The number of polynomials $t^3-t^2+at+b\in F$ with* $\max(|a|^{1/2},|b|^{1/3})\le H$

is equal to

$$CH^2 \log H + \left(C \log \sqrt{3} + D - \frac{\pi}{3\sqrt{3}} \right) H^2 + O_\varepsilon(H^{1+\varepsilon})$$

as $H \to \infty$, where

$$C = \frac{4\pi^2}{81} \prod_{q \equiv 2 \pmod 3} \left(1 - \frac{1}{q^2}\right) \prod_{p \equiv 1 \pmod 3} \left(1 - \frac{3}{p^2} + \frac{2}{p^3}\right)$$

and

$$\frac{D}{C} = 2\gamma + \log(2\pi) - 3\log\left(\frac{\Gamma(1/3)}{\Gamma(2/3)}\right) + \frac{9}{8}\log 3 + \frac{9}{4} \sum_{q \equiv 2 \pmod 3} \frac{\log q}{q^2 - 1} + \frac{27}{4} \sum_{p \equiv 1 \pmod 3} \frac{(p+1)\log p}{p^3 - 3p + 2}.$$

Theorem 5.2. *For any $H \geq 1$ let $E_H \subset \mathbb{R}^2$ be the ellipse defined by*

$$E_H : x^2 + y^2 + xy - x - y = \tfrac{1}{3}(H^2 - 1).$$

If $t^3 - t^2 + at + b \in F$ then $a \leq 0$. Fix $a \in \mathbb{Z}_{\leq 0}$. The number of polynomials of the form $t^3 - t^2 + at + b \in F$ for any $b \in \mathbb{Z}$ is equal to

$$\frac{1}{2} \sum_{d \mid (1-3a)} 3^{\omega(P_1(d))} (-1)^{\Omega(P_2(d))} - \frac{1}{6} \# E_{\sqrt{1-3a}}(\mathbb{Z})$$

where $P_j(d)$ denotes the largest divisor of d only divisible by primes $\equiv j \pmod 3$, and $\omega(n)$ (resp. $\Omega(n)$) denotes the number of prime factors of a positive integer n counted without (resp. with) multiplicity.

To prove these theorems we relate the polynomial counting problem to an integral Diophantine problem on a certain singular toric surface and then solve the Diophantine problem.

5.1 Orbit parametrizations for G-algebras

Let G be a finite group and let S be a commutative ring on which G acts by automorphisms. We say that G acts freely on S if G acts (set-theoretically) freely on $\mathrm{Hom}(S, k)$ for any field k.

Definition 5.3 (G-algebra)**.** Set $R = S^G$. We say S/R is an étale G-algebra if G acts freely on S. We say S/R is a (generically étale) G-algebra if G acts freely on $S[\Delta^{-1}]$ for some $\Delta \in R$ which is a non-zero-divisor on S.

Note that S/R is an étale G-algebra if and only if $\operatorname{Spec} S \to \operatorname{Spec} R$ is a G-torsor.

We will construct an orbit parametrization for G-algebras. Unfortunately it is basically never prehomogeneous, but it has the merit of being uniform in G.

This parametrization was found in joint work with Julian Rosen, and also independently by Fabian Gundlach.

An element of a G-algebra S/R is normal if it is trace-one and its G-conjugates form an R-module basis for S/R.

Normal elements may or may not exist — e.g. S may not be free — but the trace-one condition is not restrictive. (Easy exercise: if the G-conjugates of x form a basis of S/R, then the trace of x is in $R^\times$.)

Let $\mathbb{P}(\mathrm{reg}) = \operatorname{Proj} \mathbb{Z}[X_g : g \in G]$ be the projective space of lines in the regular representation of G. The unit group of G is the reductive group scheme $\mathcal{G}$ over $\mathbb{Z}$ whose R-points are given by

$$\mathcal{G}(R) = \left\{ \sum_{g \in G} a_g[g] \in RG^\times : \sum_{g \in G} a_g = 1 \right\}.$$

For example, as a group scheme fibered over $x \in \operatorname{Spec} \mathbb{Z}$, one can show that $\mathcal{G}_{C_2,x}$ is $\mathbb{G}_{m,x}$ for all $x \neq \operatorname{Spec} \mathbb{F}_2$ while $\mathcal{G}_{C_2,\mathbb{F}_2} = \mathbb{G}_{a,\mathbb{F}_2}$.

The unit group of G can be identified with an open affine subset of $\mathbb{P}(\mathrm{reg})$:

$$\begin{aligned} \mathcal{G} = \{\Delta \text{ is invertible}\} &\subset \mathbb{P}(\mathrm{reg}) \\ u &\mapsto \operatorname{span}(u) \end{aligned}$$

where

$$\Delta(X) = \det(X_{gh})_{g,h}$$

is the group determinant of G.

The augmentation-one condition $\sum_{g \in G} a_g = 1$ can be thought of as de-homogenizing w.r.t. the coordinate $\sum_{g \in G} X_g$ and corresponds to our trace-one condition on normal elements.

Theorem 5.4 (Gundlach 2020, O.–Rosen 2020)**.** *The R-points of the affine homogeneous scheme $\mathcal{G}/G$ are naturally in correspondence with isomorphism classes of pairs $(S/R, x)$ where S/R is an étale G-algebra and $x \in S$ is a normal element.*

We now prove this theorem.

Lemma 5.5. *The mapping $\varphi \mapsto \varphi(X_1)$ is a bijection from the set of G-equivariant ring homomorphisms $\varphi\colon \mathcal{O}(\mathcal{G}) \to S$ to the set of normal elements of S/R.*

Proof. There is a bijection from the set of G-equivariant ring homomorphisms $\varphi\colon \mathbb{Z}[X_g : g \in G] \to S$ to the set of elements of S, given by $\varphi \mapsto \varphi(X_1)$, since the values of φ on the other coordinates are uniquely determined by equivariance.

Write $x = \varphi(X_1)$. The homomorphism φ extends to $\mathbb{Z}[X_g : g \in G][\Delta^{-1}]$ if and only if

$$\varphi(\Delta)^2 = \det(gh(x))_{g,h}^2 \overset{\text{def}}{=} \operatorname{disc}(\{gx\}_g) \in S^\times.$$

We claim that $\varphi(\Delta)^2 \in S^\times$ if and only if $\{gx\}_g$ is a basis of S/R.

The property of being invertible is local, so we may assume S/R has a basis $(b_k)_k$. Writing $gx = \sum_k a_{gk} b_k$ for $a_{gk} \in R$ we have

$$\det\left(gh(x)\right)_{g,h}^2 = \det(\operatorname{tr}_{S/R}(g(x)h(x))_{g,h}) = \det(\operatorname{tr}_{S/R}(b_g b_h)_{g,h}) \det(a)^2.$$

Thus $\varphi(\Delta)^2 \in S^\times$ if and only if $\det(a) \in S^\times$ and the claim is shown.

The homomorphism φ factors through $\mathbb{Z}[X_g : g \in G][\Delta^{-1}] \to \mathcal{O}(\mathcal{G})$ if and only if φ kills $1 - \sum_g X_g$, which occurs if and only if $\operatorname{tr}_{S/R}(x) = 1$. □

Proof of Theorem. For any ring R, define the set

$$\mathfrak{M}(R) = \{\text{isom. classes of pairs } (S, x) : S/R \text{ étale } G\text{-algebra}, x \in S \text{ normal}\}.$$

We will demonstrate the existence of bijections $\mathfrak{M}(R) \cong V(R)$ which are functorial in R.

The subgroup $G \subset \mathcal{G}$ acts freely on $\mathcal{G}$, and therefore the scheme-theoretic quotient $\mathcal{G}/G$ represents the stack-theoretic quotient $[\mathcal{G}/G]$.

By definition of the stack-theoretic quotient, the R-points of $[\mathcal{G}/G]$ are pairs

$$(\operatorname{Spec} S \to \operatorname{Spec} R, \;\; \psi\colon T \to \mathcal{G})$$

where $\operatorname{Spec} S \to \operatorname{Spec} R$ is a G-torsor and $\psi\colon T \to \mathcal{G}$ is a G-equivariant morphism.

By the lemma, such pairs correspond to pairs $(S/R, x)$ where $x = \psi^*(X_1)$ is a normal element of S/R and we obtain a bijection $\mathfrak{M}(R) \cong (\mathcal{G}/G)(R)$. □

For an elementary (and longer) proof without stacks, see my paper with Julian Rosen.

5.2 Twists of G-algebras

We take $G = C_3$, and let $T = \mathcal{G}/G$. This homogeneous scheme is a torus since G is abelian. We have shown that

$$T(\mathbb{Q}) \cong \{(K/\mathbb{Q}\ C_3\text{-algebra},\ x \text{ normal})\}.$$

Concretely, a *C_3-algebra $K/\mathbb{Q}$* is a $\mathbb{Q}$-algebra equipped with an action of C_3 for which there is a C_3-linear $\mathbb{Q}$-algebra isomorphism from K to either a cubic abelian number field or the split algebra $\mathbb{Q}^3$.

Using this bijection we consider the function

$$\mathrm{Char}\colon T(\mathbb{Q}) \longrightarrow \{t^3 - t^2 + at + b \in \mathbb{Q}[t]\}$$

taking a rational point $(K/\mathbb{Q}, x)$ to the characteristic polynomial of x.

Proposition 5.6. *The image of the function* Char *is the subset of polynomials which either have Galois group C_3 or split into three linear factors over $\mathbb{Q}$ with at most two being the same. If f is such a polynomial, then the number of rational points of T with characteristic polynomial f is given by*

$$w_f = \begin{cases} 1 & \textit{if } f \textit{ has a double root,} \\ 2 & \textit{otherwise.} \end{cases}$$

Moreover, a rational point P of T is D_0-integral if and only if the associated characteristic polynomial $t^3 - t^2 + at + b$ is integral.

Proof. It is an easy exercise to show that $x = (a, b, c) \in \mathbb{Q}^3$ is normal if and only if a, b, c are not all equal, and this proves the first claim.

For the second claim, first suppose K is a cubic abelian field. Then K, equipped with its canonical Galois action, is a C_3-algebra. The twist K' of the C_3-algebra K by the outer automorphism $g \mapsto g^{-1}$ of C_3 (with twisted action $g * x = g^{-1}x$) is not isomorphic to K as a

C_3-algebra.[5] So $(K/\mathbb{Q}, x)$ and $(K'/\mathbb{Q}, x)$ are two rational points with the same characteristic polynomial.

Now suppose $K = \mathbb{Q}^3$. Any transposition gives an isomorphism of C_3-algebras from K to its twist K' by the outer automorphism of C_3. The pairs (K, x) and (K', x) are equivalent if and only if x has exactly two identical coordinates (swapping the identical coordinates gives the required isomorphism); in particular, if x has distinct coordinates then (K, x) and (K', x) determine different rational points of $\mathcal{G}/C_3$ (even though K and K' are isomorphic as C_3-algebras!).

For the third claim, at least one direction is easy: the coefficients a and b of f are the values at $(K/\mathbb{Q}, x)$ of the C_3-invariant polynomials $e_2(X/\varepsilon, Y/\varepsilon, 1-X/\varepsilon-Y/\varepsilon)$ and $-e_3(X/\varepsilon, Y/\varepsilon, 1-X/\varepsilon-Y/\varepsilon)$ in $\mathbb{Z}[X/\varepsilon, Y/\varepsilon]^{C_3} = \mathcal{O}(S_{\mathbb{Z}} - D_0)$. The other direction is more work and omitted here (see [BO23, Prop. 3]). □

5.3 An unexpected isomorphism

The tori $\mathcal{G}$ and $T = \mathcal{G}/C_3$ *happen* to be isomorphic (over $\mathbb{Q}$)! They are both isomorphic to $R^E_{\mathbb{Q}}\mathbb{G}_m$ where $E = \mathbb{Q}(\sqrt{-3})$.

One can write down a (reasonably) natural isomorphism between them. We arrive at the rather strange conclusion that there is a natural bijection

$$\mathbb{Q}(\sqrt{-3})^\times \cong \{(K/\mathbb{Q}, x) : G(K/\mathbb{Q}) \cong C_3,\ x \text{ normal}\}.$$

One can prove the following precise result. Let $\zeta = e^{2\pi i/3}$.

Theorem 5.7. *If $u + v\zeta \in \mathbb{Q}(\sqrt{-3})^\times$ has norm N and trace T then the characteristic polynomial of the corresponding rational point $(K/\mathbb{Q}, x)$ is*

$$f = t^3 - t^2 + \tfrac{1}{3}(1-N)t + \tfrac{1}{27}(1 + N(T-3)) \in \mathbb{Q}[t].$$

Such a polynomial either has Galois group C_3 or splits into three linear factors over $\mathbb{Q}$, with at most two linear factors being the same. Conversely, a monic trace-one polynomial $f = t^3 - t^2 + at + b \in \mathbb{Q}[t]$ which either has Galois group C_3 or splits into three linear factors

[5] In terms of Galois cohomology, the non-cohomologous 1-cocycles in $H^1(\mathbb{Q}, C_3)$ corresponding to the C_3-algebras K and K' have the same image under the canonical map $H^1(\mathbb{Q}, C_3) \to H^1(\mathbb{Q}, S_3)$ because the outer automorphism of C_3 is realized by S_3-conjugation.

over $\mathbb{Q}$, with at most two linear factors being the same, can be expressed in this way for precisely two rational points of T if f has no repeated roots, or for precisely one rational point of T if f has a double root which is not a triple root. The elements $u+v\zeta \in \mathbb{Q}(\sqrt{-3})^\times$ corresponding to f will be the roots of the quadratic polynomial

$$g = t^2 - \left(3 - \frac{1-27b}{1-3a}\right) t + 1 - 3a \in \mathbb{Q}[t].$$

The polynomial f will have integral coefficients if and only if

$$\begin{cases} u^2+v^2-uv \in 1+3\mathbb{Z} \text{ and} \\ (u^2+v^2-uv)(3-2u+v) \in 1+27\mathbb{Z}. \end{cases}$$

Moreover, setting $H(f) \coloneqq \sqrt{1-3a}$, we have the following discriminant relation:

$$\operatorname{disc}(g) \cdot H(f)^4 = -3^3 \cdot \operatorname{disc}(f).$$

This parametrization (specifically the characterization of integrality) will end up being important for evaluating the multiplicative Poisson summation formula.

5.4 An integral Diophantine problem

Let us state our solution to the integral Diophantine problem.

Let $\mathbb{A}^3 = \operatorname{Spec}\mathbb{Q}[X,Y,Z]$ and $\mathbb{P}_2 = \mathbb{P}(\mathbb{A}^3) = \operatorname{Proj}\mathbb{Q}[X,Y,Z]$ be equipped with the regular action of C_3. Consider the quotient surface

$$S = \mathbb{P}_2/C_3.$$

One can show that S is a *toric compactification* of T.

Let D_0 be the divisor $\{\varepsilon \coloneqq X+Y+Z = 0\} \subset S$. A rational point P of $S - D_0$ is D_0-*integral* if every regular function in $\mathcal{O}(S_\mathbb{Z} - D_0) = \mathbb{Z}[X/\varepsilon, Y/\varepsilon]^{C_3}$ is $\mathbb{Z}$-valued on P. Note that $T \subset S - D_0$.

Cubic f	Quadratic g	$\mathrm{disc}(f)$	$\mathrm{disc}(g)$	$H(f)^2$
$t^3 - t^2$	$t^2 - 2t + 1$	0	0	1
$t^3 - t^2 - t + 1$	$t^2 + 4t + 4$	0	0	4
$t^3 - t^2 - 2t + 1$	$t^2 + t + 7$	7^2	$-1 \cdot 3^3$	7
$t^3 - t^2 - 2t$	$t^2 - \frac{20}{7}t + 7$	$2^2 \cdot 3^2$	$-1 \cdot 2^2 \cdot 3^5 \cdot 7^{-2}$	7
$t^3 - t^2 - 4t + 4$	$t^2 + \frac{70}{13}t + 13$	$2^4 \cdot 3^2$	$-1 \cdot 2^4 \cdot 3^5 \cdot 13^{-2}$	13
$t^3 - t^2 - 4t - 1$	$t^2 - 5t + 13$	13^2	$-1 \cdot 3^3$	13
$t^3 - t^2 - 5t - 3$	$t^2 - 8t + 16$	0	0	16
$t^3 - t^2 - 6t + 7$	$t^2 + 7t + 19$	19^2	$-1 \cdot 3^3$	19
$t^3 - t^2 - 6t$	$t^2 - \frac{56}{19}t + 19$	$2^2 \cdot 3^2 \cdot 5^2$	$-1 \cdot 2^2 \cdot 3^5 \cdot 5^2 \cdot 19^{-2}$	19
$t^3 - t^2 - 8t + 12$	$t^2 + 10t + 25$	0	0	25
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$t^3 - t^2 - 190t + 719$	$t^2 + 31t + 571$	$7^2 \cdot 571^2$	$-1 \cdot 3^3 \cdot 7^2$	571
$t^3 - t^2 - 190t - 800$	$t^2 - \frac{23312}{571}t + 571$	$2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 13^2$	$-1 \cdot 2^2 \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 571^{-2}$	571
$t^3 - t^2 - 192t + 720$	$t^2 + \frac{17710}{577}t + 577$	$2^6 \cdot 3^6 \cdot 19^2$	$-1 \cdot 2^6 \cdot 3^9 \cdot 19^2 \cdot 577^{-2}$	577
$t^3 - t^2 - 192t - 171$	$t^2 - 11t + 577$	$3^4 \cdot 577^2$	$-1 \cdot 3^7$	577
$t^3 - t^2 - 196t + 1124$	$t^2 + \frac{922}{19}t + 589$	$2^4 \cdot 31^2$	$-1 \cdot 2^4 \cdot 3^3 \cdot 19^{-2}$	589
$t^3 - t^2 - 196t + 1109$	$t^2 + \frac{1483}{31}t + 589$	$7^4 \cdot 19^2$	$-1 \cdot 3^3 \cdot 7^4 \cdot 31^{-2}$	589
$t^3 - t^2 - 196t + 539$	$t^2 + \frac{673}{31}t + 589$	$7^2 \cdot 19^2 \cdot 37^2$	$-1 \cdot 3^3 \cdot 7^2 \cdot 31^{-2} \cdot 37^2$	589
$t^3 - t^2 - 196t + 349$	$t^2 + 13t + 589$	$3^4 \cdot 19^2 \cdot 31^2$	$-1 \cdot 3^7$	589
$t^3 - t^2 - 196t + 196$	$t^2 + \frac{3526}{589}t + 589$	$2^4 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 13^2$	$-1 \cdot 2^4 \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 19^{-2} \cdot 31^{-2}$	589
$t^3 - t^2 - 196t - 704$	$t^2 - \frac{20774}{589}t + 589$	$2^4 \cdot 3^6 \cdot 5^2 \cdot 7^2$	$-1 \cdot 2^4 \cdot 3^9 \cdot 5^2 \cdot 7^2 \cdot 19^{-2} \cdot 31^{-2}$	589

Figure 3: Some $f \in \mathbb{Z}[t]$ with Galois group C_3 and the characteristic polynomials $g \in \mathbb{Q}[t]$ of their corresponding elements in $\mathbb{Q}(\sqrt{-3})$.

Theorem 5.8. *For a certain canonical height function H on S, we have*

$$\sum_{\substack{P \in T(\mathbb{Q}),\\ D_0\text{-integral}}} H(P)^{-s} = \left(1 - \frac{1}{3^z}\right)^2 \zeta_{\mathbb{Q}(\sqrt{-3})}(z)^2 \prod_{q \equiv 2 \pmod 3} \left(1 - \frac{1}{q^{2z}}\right) \prod_{p \equiv 1 \pmod 3} \left(1 - \frac{3}{p^{2z}} + \frac{2}{p^{3z}}\right)$$

where $z = \frac{s}{2}$ and $\zeta_{\mathbb{Q}(\sqrt{-3})}$ is the Dedekind zeta function of $\mathbb{Q}(\sqrt{-3})$. This height zeta function can be meromorphically continued to the half-plane $\mathrm{Re}(s) > 1$ and its only pole in this region is at $s = 2$ with order 2. If $n \in \mathbb{Z}_{\geq 1}$ is not divisible by 3, then the number of D_0-integral rational points on T with height $\sqrt{n}$ is equal to

$$\sum_{d \mid n} 3^{\omega(P_1(d))} (-1)^{\Omega(P_2(d))}.$$

5.5 Toric height functions

It would not be possible to obtain a nice closed expression for $\sum H(P)^{-s}$ if one used a standard height function such as the max of the absolute values of the coordinates.

We briefly explain the theory of canonical heights on toric varieties, first introduced by [BT95]. Let $S = \mathbb{P}_2/C_3$ be our toric surface, and suppose we are given a morphism $\phi\colon S \to \mathbb{P}_N$. This gives us a height on S:

$$\begin{aligned} H_\phi\colon S(\mathbb{Q}) &\to \mathbb{R}_{>0} \\ P &\mapsto H_\phi(P) = H_{\mathbb{P}_N}(\phi(P)) \end{aligned}$$

where $H_{\mathbb{P}_N}$ is the standard height function on $\mathbb{P}_N$.

To obtain a nicer height, we *diagonalize* this morphism for the action of T.

Let V denote the (finite-dimensional) vector space of rational functions v on S of the form

$$v = \phi^* s = s \circ \phi$$

where s is any linear homogeneous function in the $N+1$ projective coordinates on $\mathbb{P}_N$. The space V is naturally a representation of T:

$$(t \cdot v)(P) = v(t^{-1}P).$$

Since T is abelian, we may diagonalize its action on V. Suppose that $v_0, \ldots, v_N \in V$ are weight vectors which form a basis, and use these as coordinates for a new morphism ϕ_v:

$$\phi_v(P) = [v_0(P) : \cdots : v_N(P)].$$

Since ϕ and ϕ_v are related by an automorphism of $\mathbb{P}_N$, their height functions are equivalent, i.e.

$$\log H_\phi = \log H_{\phi_v} + O(1).$$

The morphism ϕ_v is equivariant, i.e. there is a homomorphism $\psi\colon T \to \mathbb{G}_m^{N+1}$ (the weights of the weight basis) such that $\phi_v(t \cdot P) = \psi(t)\phi_v(P)$.

Definition 5.9. A toric height function on S is a height of the form H_ϕ for some equivariant morphism $\phi\colon S \to \mathbb{P}_N$.

By a direct computation, one can prove the following.

Lemma 5.10. *There is an equivariant morphism $\phi\colon S \to \mathbb{P}_3$ (defined over $\mathbb{Q}(\sqrt{-3})$) whose* *coordinates are the following four weight vectors:*

$$e_1^3, \quad e_1^3 - 3e_2e_1, \quad e_1^3 - \tfrac{9}{2}e_1e_2 + \tfrac{27}{2}e_3 + \tfrac{\sqrt{-27}}{2}\sqrt{\mathrm{disc}}, \quad e_1^3 - \tfrac{9}{2}e_1e_2 + \tfrac{27}{2}e_3 - \tfrac{\sqrt{-27}}{2}\sqrt{\mathrm{disc}}$$

where $\sqrt{\mathrm{disc}} = (X-Z)(Y-X)(Z-Y)$ *and* e_1, e_2, e_3 *are the elementary symmetric functions in* X, Y, Z*. Let* H_0 *be the toric height on* S *associated to this equivariant morphism. If* $(K/\mathbb{Q}, x)$ *is a* D_0*-integral rational point of* T*, then*

$$H_0(K/\mathbb{Q}, x) = (1-3a)^{3/2}$$

where $t^3 - t^2 + at + b = \mathrm{Char}(K/\mathbb{Q}, x)$*.*

One can show that $H = H_0^{1/3}$ is equivalent to the "root height" $\max(|a|^{1/2}, |b|^{1/3})$.

Toric height functions can be canonically extended to *adelic* height functions. This means that there are *local* height functions

$$H_v \colon T(\mathbb{Q}_v) \to \mathbb{R}_{>0}$$

such that the product defines a *global (adelic)* height function on $T(\mathbb{A})$,

$$H = \prod_v H_v \colon T(\mathbb{A}) \to \mathbb{R}_{>0},$$

whose restriction to $T(\mathbb{Q}) \subset T(\mathbb{A})$ is the original toric height.

Since the condition of being integral is a local condition, it is also possible to define a locally constant function $\mathbf{1} = \mathbf{1}_{D_0}$ on $T(\mathbb{A})$ such that

$$\mathbf{1}((t_v)_v) = \begin{cases} 1 & \text{if } v = p \text{ finite and } \phi(t_p) \in \mathbb{Z}_p \text{ for any } \phi \in \mathcal{O}(S_{\mathbb{Z}} - D_0), \\ 0 & \text{otherwise.} \end{cases}$$

Adelic multiplicative Poisson summation

We would like to exploit the fact that the Dirichlet series

$$Z(s) = Z(e; s) = \sum_{\substack{P \in T(\mathbb{Q}), \\ D_0\text{-}integral}} H(P)^{-s} = \sum_{P \in T(\mathbb{Q})} \mathbf{1}(P) H(P)^{-s}$$

can be regarded as the value at $x = e$ of an automorphic function on $T(\mathbb{A})$:

$$Z(x; s) = \sum_{P \in T(\mathbb{Q})} \mathbf{1}(xP) H(xP)^{-s}.$$

For this purpose we will make use of an abstract form of the Poisson summation formula. Let B be a locally compact abelian group with Haar measure db. Let $f \in L^1(B)$. The Fourier transform of f given by

$$\widehat{f}(\chi) = \int_B f(b) \chi(b)^{-1} \, db$$

converges and defines a continuous function on $B^\vee$.

Now let A be a closed subgroup of B and let $A^\perp \subset B^\vee$ denote the subgroup of characters on B that are trivial on A. The general Poisson summation formula — following from the classical proof for $\mathbb{Z} \subset \mathbb{R}$ — says that if $\widehat{f}|_{A^\perp} \in L^1(A^\perp)$ then

$$\int_A f(ab) \, da = \int_{A^\perp} \widehat{f}(\chi) \chi(b) \, d\chi$$

for a.e. $b \in B$ and suitably normalized Haar measure on $A^\perp$ [Fol95, Theorem 4.4.2, p. 105].

We apply this to the *discrete* (and hence closed) subgroup $T(\mathbb{Q}) \subset T(\mathbb{A})$ to obtain a formula for the integral of f over $T(\mathbb{Q})$:

$$\int_{T(\mathbb{Q})} f(xy) \, dx = \int_{T(\mathbb{Q})^\perp} \widehat{f}(\chi) \chi(y) \, d\chi = \int_{(T(\mathbb{Q}) \backslash T(\mathbb{A}))^\vee} \widehat{f}(\chi) \chi(y) \, d\chi$$

for a.e. $y \in T(\mathbb{Q})$ and suitably normalized Haar measure $d\chi$ on $T(\mathbb{Q})^\perp$ [Fol95, Theorem 4.4.2, p. 105].

We take f to be

$$x \mapsto f(x) = H(x, -s, D_0) = H(x)^{-s} \mathbf{1}(x) \qquad (x \in T(\mathbb{A})).$$

The function $H(x, -s, D_0)$ is factorizable so its Fourier transform is equal to the product of the transforms of its local factors:

$$\widehat{H}(\chi, -s, D_0) = \prod_{v \in M_{\mathbb{Q}}} \widehat{H_v}(\chi_v, -s, D_0).$$

Note that in Tate's thesis, Poisson summation is applied *additively* for the discrete subgroup $E \subset \mathbb{A}_E$. While $\mathbb{A}_E$ is self-dual, the multiplicative group $T(\mathbb{A})$ is not self-dual, so we will need to work harder to compute the Fourier transform in our multiplicative setting. (Recall that class field theory seeks to describe the automorphic characters of $T(\mathbb{A})$ when $T = R^E_{\mathbb{Q}}\mathbb{G}_m$.)

5.6 Proof of Theorem 5.8

We must describe automorphic forms on T, i.e. elements of the dual of the automorphic quotient $T(\mathbb{Q})\backslash T(\mathbb{A})$. This is well-known. Our function $H(x, -s, D_0)$ is invariant under the action of an open compact subgroup K (of index six in the maximal compact subgroup), so we need only describe automorphic forms of level K, i.e. $(T(\mathbb{Q})\backslash T(\mathbb{A})/K)^\vee$.

Recall the "unexpected isomorphism" $\alpha\colon T \xrightarrow{\sim} R^E_{\mathbb{Q}}\mathbb{G}_m$. We obtain a continuous family of such automorphic forms as follows:

$$\chi_t(x) = |N^E_{\mathbb{Q}}(\alpha x)|^{t/2}_{\mathbb{A}_E}.$$

One can then prove that

$$(T(\mathbb{Q})\backslash T(\mathbb{A})/K)^\vee = \{\chi_t : t \in \mathbb{R}\} \cong \mathbb{R}$$

which amounts to showing that the ray class group for E (with modulus $3O_E = \alpha(K)$) is trivial.

Each local Fourier transform can be computed explicitly. The archimedean Fourier transform $\widehat{H_\infty}(\chi_t, -s, D_0)$ is a certain rational function in t and s, and $\widehat{H_p}(\chi_t, -s, D_0)$ is a power series in p^s.

To evaluate the right-hand side of the Poisson formula, one multiplies together these local Fourier transforms and then integrates over the automorphic forms χ_t using Cauchy's residue formula:

$$\begin{aligned}\int_{(T(\mathbb{A})/T(\mathbb{Q}))^\vee} \widehat{H}(\chi, -s, D_0)\, d\chi &= \int_{(T(\mathbb{A})/T(\mathbb{Q})/K)^\vee} \widehat{H}(\chi, -s, D_0)\, d\chi \\ &= \int_{\mathbb{R}} \widehat{H}(\chi_t, -s, D_0)\, dt = \left(\frac{-1}{2\pi i}\right)\frac{3s}{2\pi i}\sum_\eta \eta^{-s}\int_{\mathbb{R}} \frac{\chi_t(\eta)^{-1}\, dt}{(t + \frac{s}{2\pi i})(t - \frac{s}{\pi i})} \\ \text{(Cauchy's residue formula)} &= \sum_\eta \eta^{-s}\chi_{\frac{s}{2\pi i}}(\eta).\end{aligned}$$

Here $\eta \in T(\mathbb{A}^f)/K^f_{\max} \xrightarrow{\alpha} \mathrm{FracId}(E)$ may be regarded (via α) as an (integral) ideal of O_E satisfying certain local conditions dictated by the local behavior of T (which can be seen in its associated Galois representation). Expressing these local conditions and rearranging some Euler factors obtains the theorem.

(Note that the very fact that η can be described by *local* conditions means that $Z(s)$ has an Euler product.)

By means of standard Tauberian methods, one obtains from $Z(s)$ a (weighted) count for possibly reducible C_3-polynomials. To obtain Theorem 5.1 one subtracts off the count of reducible polynomials (which correspond to integral points on a certain ellipse parametrizing all trace-one points in Minkowski space with a given height). This is not difficult.

A refinement: the number of trace-one generators of a given cubic abelian field

To prove the formula for $Z(s)$, and hence the count for abelian cubics, it sufficed to use the *untwisted* Poisson formula (i.e. $y = 1$). By making use of the twisting parameter, it is possible to obtain a refined formula which counts the number of monic trace-one abelian cubics which generate a *fixed* cubic abelian field.

Fix an abelian cubic number field K which is tamely ramified over $\mathbb{Q}$ and let F_K denote the set of polynomials of the form $t^3 - t^2 + at + b \in \mathbb{Z}[t]$ whose associated root field is K. Recall that for such polynomials we necessarily have $a \leq 0$ and we set $H(t^3 - t^2 + at + b) = \sqrt{1 - 3a}$ ("toric height").

Theorem 5.11. *Let D_K denote the discriminant of K. We have that*

$$\sum_{f \in F_K} H(f)^{-2s} = D_K^{-s}(1 - 3^{-s})\zeta_{\mathbb{Q}(\sqrt{-3})}(s).$$

If $t^3 - t^2 + at + b \in F_K$ then $a \leq 0$ and D_K divides $1 - 3a$. Fix $a \in \mathbb{Z}_{\leq 0}$. The number of polynomials of the form $t^3 - t^2 + at + b \in F_K$ for any $b \in \mathbb{Z}$ is equal to the number of integral ideals in $\mathbb{Q}(\sqrt{-3})$ with norm $N = (1 - 3a)D_K^{-1}$. Explicitly,

$$\#\{\, f = t^3 - t^2 + at + b \ :\ b \in \mathbb{Z},\ K_f \cong K \,\} = \sigma_0\left(P_1\left(\frac{1 - 3a}{D_K}\right)\right).$$

where $\sigma_0(P)$ is the number of divisors of P and $P_1(N)$ is the largest divisor of N only divisible *by primes* $\equiv 1 \pmod 3$.

Remarkably, we conclude that the number of trace-one monic polynomials with a given linear coefficient that generate K is *essentially independent of K and only depends on the arithmetic of* $\mathbb{Q}(\sqrt{-3})$. This is illustrated in the table below of all trace-one monic integral cubic polynomials with $H(f) \leq 25$ which generate either $K_{49} = \mathbb{Q}(\zeta_7)^+$ or $K_{169} = \mathbb{Q}[t]/(t^3 - t^2 - 4t - 1)$.

$H(f)^2$	$f : K_f = K_{49}$
7×1	$t^3 - t^2 - 2t + 1$
7×4	$t^3 - t^2 - 9t + 1$
7×7	$t^3 - t^2 - 16t + 29,\ t^3 - t^2 - 16t - 13$
7×13	$t^3 - t^2 - 30t + 43,\ t^3 - t^2 - 30t - 41$
7×16	$t^3 - t^2 - 37t + 29$
7×19	$t^3 - t^2 - 44t + 127,\ t^3 - t^2 - 44t - 83$
7×25	$t^3 - t^2 - 58t - 13$
7×28	$t^3 - t^2 - 65t + 169,\ t^3 - t^2 - 65t - 167$
7×31	$t^3 - t^2 - 72t + 169,\ t^3 - t^2 - 72t - 41$
7×37	$t^3 - t^2 - 86t + 337,\ t^3 - t^2 - 86t - 251$
7×43	$t^3 - t^2 - 100t + 113,\ t^3 - t^2 - 100t - 181$

$H(f)^2$	$f : K_f = K_{169}$
13×1	$t^3 - t^2 - 4t - 1$
13×4	$t^3 - t^2 - 17t + 25$
13×7	$t^3 - t^2 - 30t + 25,\ t^3 - t^2 - 30t - 53$
13×13	$t^3 - t^2 - 56t + 181,\ t^3 - t^2 - 56t + 25$
13×16	$t^3 - t^2 - 69t - 131$
13×19	$t^3 - t^2 - 82t + 155,\ t^3 - t^2 - 82t - 235$
13×25	$t^3 - t^2 - 108t + 337$
13×28	$t^3 - t^2 - 121t + 545,\ t^3 - t^2 - 121t - 79$
13×31	$t^3 - t^2 - 134t - 131,\ t^3 - t^2 - 134t - 521$
13×37	$t^3 - t^2 - 160t + 467,\ t^3 - t^2 - 160t - 625$
13×43	$t^3 - t^2 - 186t + 961,\ t^3 - t^2 - 186t + 415$

The method is similar to what we did for $Z(s)$.

We explain where the twisting parameter comes from. The point is that we will approximate a rational point (K, x) on T with an adelic point y_K on $\mathcal{G}$. Let x be any normal element of K.

A classical theorem of Noether asserts that K is tamely ramified if and only if O_K admits a normal basis. If x is part of a normal integral basis, then (K, x) is in the maximal compact subgroup of $T(\mathbb{A})$.

The *existence* of a normal integral basis implies that

$$(K \otimes \mathbb{Q}_p, x) = y_p k_p$$

where $y_p \in \mathcal{G}(\mathbb{Q}_p)$ is the change of normal basis from Gx to a p-integral normal basis. Since $K/\mathbb{Q}$ is split at infinity, the real point $(K \otimes \mathbb{R}, x) \in T(\mathbb{R})$ is equal to $\pi(y_\infty)$ for some $y_\infty \in \mathcal{G}(\mathbb{R})$ where $\pi\colon \mathcal{G} \to T$ is the natural quotient morphism. Then

$$(K, x) = y_K k$$

where $y_K = (y_v)_v \in \mathcal{G}(\mathbb{A})$ and $k = (k_v)_v \in K$.

Crucially, we have $H((K,x)) = H(y_K)$, where now y_K is in $\mathcal{G}(\mathbb{A})$ rather than $T(\mathbb{A})$.

The twisted Poisson formula for $f(t) = H(t(K,x), -s, D_0)$ with $y = y_K$ implies that

$$\sum_{f \in F_K} H(f)^{-s} = \sum_{t \in \mathcal{G}(\mathbb{Q})} H(t(K,x), -s, D_0) = \int_{\mathcal{G}(\mathbb{Q})^{\perp}} \widehat{f}(\chi)\chi(y_K)\, d\chi.$$

The rest of the computation proceeds similarly with $\mathcal{G}$ in place of T.

References

[Bha07] Manjul Bhargava. Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants. *Int. Math. Res. Not. IMRN*, (17):Art. ID rnm052, 20, 2007.

[Bha08] Manjul Bhargava. Higher composition laws. IV. The parametrization of quintic rings. *Ann. of Math. (2)*, 167(1):53–94, 2008.

[Bha14] Manjul Bhargava. The geometric sieve and the density of squarefree values of invariant polynomials, 2014.

[Bha21] Manjul Bhargava. Lecture slides for *Sieves and Algebraic Number theory*, 2021.

[BO23] Shubhrajit Bhattacharya and Andrew O'Desky. On monic abelian trace-one cubic polynomials, 2023.

[BSW22a] Manjul Bhargava, Arul Shankar, and Xiaoheng Wang. Squarefree values of polynomial discriminants I. *Invent. Math.*, 228(3):1037–1073, 2022.

[BSW22b] Manjul Bhargava, Arul Shankar, and Xiaoheng Wang. Squarefree values of polynomial discriminants II, 2022.

[BT95] Victor V. Batyrev and Yuri Tschinkel. Rational points of bounded height on compactifications of anisotropic tori. *Internat. Math. Res. Notices*, (12):591–635, 1995.

[CM06] Alina Carmen Cojocaru and M. Ram Murty. *An introduction to sieve methods and their applications*, volume 66 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2006.

[Eke91] Torsten Ekedahl. An infinite version of the Chinese remainder theorem. *Comment. Math. Univ. St. Paul.*, 40(1):53–59, 1991.

[Fol95] Gerald B. Folland. *A course in abstract harmonic analysis*. Studies in Advanced Mathematics. CRC Press, Boca Raton, FL, 1995.

[Gra98] Andrew Granville. *ABC* allows us to count squarefrees. *Internat. Math. Res. Notices*, (19):991–1009, 1998.

[Gre92] George Greaves. Power-free values of binary forms. *Quart. J. Math. Oxford Ser. (2)*, 43(169):45–65, 1992.

[Hoo68] Christopher Hooley. On the square-free values of cubic polynomials. *J. Reine Angew. Math.*, 229:147–154, 1968.

[Liu16] H.-Q. Liu. On the distribution of squarefree numbers. *J. Number Theory*, 159:202–222, 2016.

[Ser78] Jean-Pierre Serre. Une “formule de masse” pour les extensions totalement ramifiées de degré donné d’un corps local. *C. R. Acad. Sci. Paris Sér. A-B*, 286(22):A1031–A1036, 1978.

[Ser97] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem.* Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997.

[WY92] David J. Wright and Akihiko Yukie. Prehomogeneous vector spaces and field extensions. *Invent. Math.*, 110(2):283–314, 1992.