Counting number fields of bounded discriminant

David Lowry-Duda

Maine–Québec Number Theory Conference, October 2022

ICERM
Brown University

Acknowledgements

This project grew out of a workshop at AIM on *Arithmetic statistics, discrete reduction, and Fourier analysis* in February of last year.

This talk includes work done in collaboration with Theresa Anderson, Ayla Gafni, Kevin Hughes, Robert Lemke Oliver, Frank Thorne, Jiuya Wang, and Ruixiang Zhang.

Broad Strategy

Our goal is to count the number $N_n(X)$ of degree n number fields over $\mathbb{Q}$ with discriminant up to X. At their core, almost all general techniques to count number fields resort to estimating the size of a family of polynomials guaranteed to generate all number fields with discriminant up to X.

We use the same initial setup: to count $N_n(X)$, we count monic polynomials

$$f(x) = x^n + c_1 x^{n-1} + \cdots + c_n.$$

It will be convenient to introduce an auxiliary notation

$$H = X^{\frac{1}{2n-2}}$$

and refer to polynomials with $|c_i| \leq H^i$ as having height at most H.

Schmidt [Sch95] showed that it suffices to count irreducible polynomials f with trace 0 (i.e. with $c_1 = 0$) and height[1] at most H. This leads to the bound

$$N_n(X) \ll H^{2+\cdots+n} \asymp X^{\frac{n+2}{4}}.$$

We call this the Schmidt Bound.

It's not hard to show that including polynomials that don't have trace 0 causes no problems. This naively adds a factor of H (as we count over $|c_1| \leq H^1$) — but this family overcounts also by a factor of at least H.

Lemma

The cardinality of the set of monic irreducible polynomials of height H bounds $H \cdot N_n(X)$. To bound $N_n(X)$, we can count these polynomials and divide by H.

[1] roughly, ignoring here and later constants that might depend on n

There is a folklore conjecture, sometimes attributed to Linnik, that the true answer is closer to

$$N_n(X) \asymp X.$$

Proving this is classical for $n = 2$. For $n \leq 5$, this is known and due to Davenport and Heilbronn ($n = 3$) and Bhargava ($n = 4, 5$). But otherwise this is unknown.[2]

For $n \gg 1$, Ellenberg and Venkatesh, Couveignes, and Lemke Oliver and Thorne (three separate papers, each improving over the previous) proved that

$$N_n(X) \ll X^{c(\log n)^2}.$$

Computing constants, this improves on Schmidt's bound for $n \gtrsim 95$.

Recent work of Bhargava, Shankar, and Wang (appearing simultaneously on the arxiv as our preprint) uses different techniques to get a better bound than I present here.

[2] It is also interesting to ask about $N_n(X; G)$ for a specific Galois group G. This is also studied.

Sources of Loss

Counting all polynomials of height $H \asymp X^{1/(2n-2)}$ detects all number fields of discriminant up to X, but typically vastly overestimates. There are two large sources of error.

1. The typical polynomial of height H has $\mathrm{Disc}(f) \approx H^{n^2-n} = X^{\frac{n}{2}}$, and typically cuts out a number field with similar discriminant. Thus we are including many, many extraneous polynomials by including all polynomials of height up to H.
2. Overcounting: the same number field might be counted repeatedly.

Ellenberg and Venkatesh recognized that relevant polynomials have other associated data (essentially mixed traces $\mathrm{Tr}(\alpha^i \beta^j)$ of small height), allowing them to discard extraneous polynomials for $n \gg 1$. In this work we identify different extraneous polynomials, ultimately based on harmonic analytic properties of the discriminant function.

To count polynomials, we split them into two pieces:

1. We first count polynomials with ‘small’ discriminant, and then
2. We count polynomials with ‘large’ discriminant.

Most polynomials have large discriminant. If $f(x)$ cuts out the K, then

$$\mathrm{Disc}(f) = \mathrm{Disc}(K)[\mathcal{O}_K : \mathbb{Z}[\alpha]]^2,$$

where α is a root of f over K. We call the last factor $\mathrm{Index}(f)^2$. In order to bound the number of polynomials with large discriminant, we split these into two subpieces, depending on whether the radical of the index is small or large.

1. We first count polynomials with ‘small’ discriminant, and then
2. 2.1 We then count polynomials with ‘large’ discriminant and ‘large’ index radical.
   2.2 We then count polynomials with ‘large’ discriminant and ‘small’ index radical.

Small discriminant

For polynomials of small discriminant, we appeal to Davenport's Lemma (or the Lipschitz Principle).

Lemma (Davenport's Lemma)

Suppose $\Omega \subset \mathbb{R}^n$ is a region cut out by algebraic inequalities. Then the number of lattice points $\mathbb{Z} \cap \Omega$ is

$$\mathrm{Vol}(\Omega) + O\big(\max_{\pi} \mathrm{Vol}(\pi(\Omega))\big),$$

where the maximum runs over projections π of $\mathbb{R}^n$ onto its various coordinate hyperplanes.

Morally, the number of lattice points in a region is the volume of the region, up to an error comparable to the *surface area* of the region (appropriately defined).

We define our region to be

$$\Omega_{H,Y} := \{(c_1, \ldots, c_n) \in \mathbb{R}^n : |c_i| \leq H^i, \mathsf{Disc}(f_c) \leq H^{n^2-n}/Y\}.$$

We will freely translate between $\mathbf{c} \in F^n$ and monic polynomials in $F[x]$, via

$$f_c(x) = x^n + c_1 x^{n-1} + \cdots + c_n.$$

The maximum volume of coordinate projections is trivially $O_n(H^{\frac{n^2+n}{2}-1})$, coming from projecting $(c_1, \ldots, c_n) \mapsto (c_2, \ldots, c_n)$ (i.e. forgetting c_1) and ignoring the discriminant condition.

It suffices to consider $\Omega_{1,Y}$, as

$$\mathrm{Vol}(\Omega_{H,Y}) = H^{\frac{n^2+n}{2}} \mathrm{Vol}(\Omega_{1,Y}),$$

It is possible to apply Van der Corput's lemma to show that $\mathrm{Vol}(\Omega_{1,Y}) \ll Y^{-\frac{1}{n-1}}$, but we do better.

Discriminant density

What is the density of the condition that the discriminant is small?

Proposition (Discriminant density)

For $n \geq 2$, let $\mathbb{Q}_v$ be a completion of $\mathbb{Q}$ with absolute value $|\cdot|_v$. Let μ_v be the associated Haar measure on $\mathbb{Q}_v$ normalized when v is finite so that $\mu_v(\mathbb{Z}_v) = 1$, and agreeing with the Lebesgue measure when v is infinite. Let ν be the product measure on $\mathbb{Q}_v^n$. For any $\delta \in (0, 1)$,

$$\nu(\{\mathbf{c} \in \mathbb{Q}_v^n : |c_i|_v \leq 1 \text{ and } |\mathrm{Disc}(f_{\mathbf{c}})|_v \leq \delta\}) \asymp_n \delta^{\frac{1}{2}+\frac{1}{n}}.$$

With $\delta = Y^{-1}$ and $\mathbb{Q}_v = \mathbb{R}$, this gives

$$\mathrm{Vol}(\Omega_{1,Y}) \ll Y^{-\frac{1}{2}-\frac{1}{n}},$$

implying that the number of polynomials of height up to H which $\mathrm{Disc}(f) \leq H^{n^2-n}/Y$ is $\ll H^{\frac{n^2+n}{2}}/Y^{\frac{1}{2}+\frac{1}{n}} + H^{\frac{n^2+n}{2}-1}$.

Sketch on discriminant density

Proving this is annoying in *coordinate space*. Working with the discriminant is much easier in *root space*. It's possible to change variables to change perspective, following work of Shankar and Tsimerman.

Briefly, let $\mathbf{1}_\delta(f)$ denote the characteristic function for polynomials with $|\mathrm{Disc}(f)|_v \leq \delta$. Then we have that

$$\nu(\cdots) = \sum_{[K_v:\mathbb{Q}_v]=n} \frac{|\mathrm{Disc}(K_v)|_v^{1/2}}{|\mathrm{Aut}(K_v)|} \int_{\mathcal{O}_{K_v}} |\mathrm{Disc}(f_\alpha)|_v^{1/2} \mathbf{1}_\delta(f_\alpha) d\mu(\alpha),$$

where the sum is over étale algebras and f_α is the characteristic polynomial of α. Pretending every étale algebra is totally split, for any α for which $\mathbf{1}_\delta(f_\alpha) \neq 0$, we have

$$|\mathrm{Disc}(f_\alpha)|_v = \prod_{i=1}^{n} \prod_{j \neq i} |\alpha_i - \alpha_j|_v \leq \delta \implies \prod_{j \neq i} |\alpha_i - \alpha_j|_v \leq \delta^{\frac{1}{n}} \text{ for some } i.$$

The $\delta^{\frac{1}{2}}$ comes from $|\mathrm{Disc}(f_\alpha)|_v^{1/2}$.

Large discriminant, large index radical

That handles small discriminant counts. For larger discriminants, we split on the radical of the index. This is inspired from an old preprint of Bhargava, Shankar, and Wang [BSW22] that proves:

Lemma (BSW-Inventiones)

For $n \geq 3, H \geq 1, M \geq 1$, we have that

$$\#\left\{ f_c : \substack{|c_i| \leq H^i \\ m^2 | \mathrm{Disc}(f_c) \text{ for some squarefree } m \geq M} \right\} \ll_n \frac{H^{\frac{n^2+n}{2}}}{M} + H^{\frac{n^2+n}{2} - \frac{1}{5}}.$$

Note that $\mathrm{Index}(f)^2 \mid \mathrm{Disc}(f)$, and if $\mathrm{Index}(f)$ is large and has large radical, then it has a large squarefree part. In our paper, we sharpen this result to $-\frac{1}{2} + \epsilon$ instead of $-\frac{1}{5}$ (by applying a stronger sieve).

Small index radical

It remains to count polynomials with large discriminant, but small index radical. We prove that

Theorem

The number of polynomials of degree n and height H for which $\mathrm{rad}(\mathrm{Index}(f)) < H^{1-\epsilon}$ but $\mathrm{Index}(f) > H^{\frac{n(n-3)}{2}}$ is $O(H^{\frac{n^2+n}{2}-\frac{4}{3}-\frac{4}{n}+\epsilon} + H^{\frac{n^2+n}{2}-\frac{2n}{3}+3+\epsilon})$.

We'll return to this later. A large part of our recent preprint works on proving this result. More broadly, suppose we had a hypothetical result for some $0 < \alpha < 1$ and $\beta > 0$:

Proposition (Proposition $P(\alpha, \beta)$)

The number of polynomials of degree n and height H for which $\mathrm{rad}(\mathrm{Index}(f)) < H^{\alpha}$ but $\mathrm{Index}(f) > H^{\frac{n(n-3)}{2}}$ is $O(H^{\frac{n^2+n}{2}-\beta+\epsilon})$.

Assembling a proof

As noted before, $\mathrm{Disc}(f) = \mathrm{Disc}(K)\,\mathrm{Index}(f)^2$. Taking $Y = H^{n-1}$ in the *small discriminant lemma* shows that the number of polynomials of height up to H and having $\mathrm{Disc}(f) \leq H^{(n-1)^2}$ is $O(H^{\frac{n^2+n}{2}-1})$. Thus with at most that many exceptions,

$$\mathrm{Index}(f)^2 \cdot \mathrm{Disc}(K) = \mathrm{Disc}(f) \geq H^{(n-1)^2}.$$

We are counting number fields K with $\mathrm{Disc}(K) \leq X \sim H^{2(n-1)}$, and thus each of the corresponding polynomials has index bounded below by

$$\mathrm{Index}(f) \gg H^{\frac{(n-1)(n-3)}{2}}.$$

Taking $M = H^\alpha$ in the BSW Lemma shows that the number of polynomials of height H, index bounded below by $H^{\frac{(n-1)(n-3)}{2}}$, and index radical bounded below by H^α is at most $H^{\frac{n^2+n}{2}-\alpha} + H^{\frac{n^2+n}{2}-\frac{1}{5}}$. And Proposition $P(\alpha, \beta)$ (if true) implies that the number of remaining polynomials (with $\mathrm{rad}(\mathrm{Index}(f)) < H^\alpha$) is at most $H^{\frac{n^2+n}{2}-\beta+\epsilon}$.

In total, these bounds imply that

$$H \cdot N_n(X) \ll H^{\frac{n^2+n}{2}-\alpha+\epsilon} + H^{\frac{n^2+n}{2}-\beta+\epsilon} + H^{\frac{n^2+n}{2}-\frac{1}{2}+\epsilon}.$$

Recalling that $H \approx X^{\frac{1}{2n-2}}$, let $\delta = \min\{\frac{1}{2}, \alpha, \beta\}$. Then this shows that

$$N_n(X) \ll X^{\frac{n+2}{4}-\frac{\delta}{2n-2}+\epsilon}.$$

In particular, *any* proved form of Proposition $P(\alpha, \beta)$ yields an improvement over Schmidt.

In our preprint, we show that we can take $\delta = \frac{1}{2}$.

In the remainder of this talk, I'd like to describe how one might try to prove propositions $P(\alpha, \beta)$ — counting the number of polynomials of height H, small index radical, and large index.

Intuitively, one first quantifies the intuition that if $\mathsf{Index}(f)$ is large but $\mathrm{rad}(\mathsf{Index}(f))$ is small, then $\mathsf{Index}(f)$ should be highly divisible by 'large' powers of primes. One can show that there is a cubefull divisor d of $\mathsf{Index}(f)$ of size $H^2 < d \leq H^3$.

Then we bound the number of polynomials of height H with $d^2 \mid \mathsf{Disc}(f)$, and take the union bound across various possible cubefull d.

To bound the number of polynomials with $d^2 \mid \mathrm{Disc}(f)$, we use Fourier analysis. Let $\psi_{p^{2k}}$ be the characteristic function for polynomials having p^{2k} dividing their discriminants and define

$$\widehat{\psi_{p^{2k}}}(\mathbf{u}) := \frac{1}{p^{2kn}} \sum_{f} \psi_{p^{2k}}(f) \exp\left(\frac{2\pi i \langle f, \mathbf{u} \rangle}{p^{2k}}\right).$$

Then our goal is to produce good bounds for $\widehat{\psi_{p^{2k}}}$ and to study its support (and then apply a form of the Chinese remainder theorem Poisson summation to recover information about $\psi_{d^{2k}}$).

Bounds

The “trivial” Fourier estimate is the density of the relevant polynomials, which follows from the discriminant density proposition earlier — not applied at finite places.

Corollary

Let $n \geq 2, k \geq 1$. The set of monic polynomials $f \in \mathbb{Z}_p[x]$ for which $p^{2k} \mid \operatorname{Disc}(f)$ has relative density $\asymp_n p^{-k-\frac{2k}{n}}$.

Thus $|\widehat{\psi}_{p^{2k}}(\boldsymbol{u})| \ll_n p^{-k-\frac{2k}{n}}$ in general. This is nontrivial, but we want better bounds. This is hard.

But it turns out there is an interesting and strange interaction between the number theoretic properties of the discriminant function and Fourier transform of $\psi_{p^{2k}}$ that helps significantly.

Support

We show that the support of $\widehat{\psi_{p^{2k}}}$ is constrained to "near arithmetic progressions." Roughly, if $\mathbf{u} = (u_1, \ldots, u_n) \in (\mathbb{Z}/p^{2k}\mathbb{Z})^n$, then $\mathbf{u}$ is in the support only if

$$\min\{v_p(u_i), k\} = \min\{v_p(u_n) + (n-i)a, k\}.$$

This is like an arithmetic progression, except that terms above k are considered k. Weird!

To prove this, we show that for all $\boldsymbol{u}$ in the support of $\widehat{\psi_{p^{2k}}}$, we have that $\boldsymbol{u} \approx \boldsymbol{D_c}$ (where $\boldsymbol{D_c} := (\partial_{c_1} \operatorname{Disc}(f_c), \ldots, \partial_{c_n} \operatorname{Disc}(f_c)))$ for some $\boldsymbol{c}$. (This is not at all obvious). The arithmetic progression property comes from studying possible gradient vectors $\boldsymbol{D_c}$. The idea then is that the discriminant polynomial satisfies an enormous number of algebraic relations.

Nontrivial bounds

For nontrivial phases $\boldsymbol{u}$, the work is technical. We briefly sketch the shape of the argument. Suppose we consider $\boldsymbol{u} = (u_1, u_2, 0, \ldots, 0)$. After applying the Shankar–Tsimerman change of variables to "root space", we want to study

$$\int_{\mathcal{O}_{K_p}} |\mathrm{Disc}(f_\alpha)|_p^{1/2} \phi_{p^{2k}}(f_\alpha) e(-u_1\sigma_1(f_\alpha) + u_2\sigma_2(f_\alpha)) d\mu(\alpha),$$

where f_α is the characteristic polynomial of α and $\sigma_i(\alpha)$ are the ith elementary symmetric function in the roots $\boldsymbol{\lambda}$ of f_α.

$|\mathrm{Disc}(f_\alpha)|_p$ is determined by congruences between the roots of f_α. We study points $\alpha \in \mathcal{O}_{K_p}$ with neighborhoods that all have "large" discriminants for congruence reasons via density. In other neighborhoods, we apply stationary phase.

It turns out that it suffices to study $\boldsymbol{u} = (u_1, u_2, 0, \dots, 0)$. To see this, we look at the fundamental Poisson argument. With $\phi(\cdot)$ a rapidly decaying positive Schwarz function that is 1 on the unit box $[-1,1]^n$, Poisson summation gives that

$$\sum_{\boldsymbol{c}} \phi(\frac{c_1}{H}, \dots, \frac{c_n}{H^n}) \psi_{d^2}(f_{\boldsymbol{c}}) = H^{\frac{n^2+n}{2}} \widehat{\phi_{p^2}}(\mathbf{0}) \widehat{\psi}_{d^2}(\mathbf{0})$$

$$+ H^{\frac{n^2+n}{2}} \sum_{\boldsymbol{u} \neq \mathbf{0}} \widehat{\psi}_{d^2}(\boldsymbol{u}) \widehat{\phi}\left(\frac{u_1 H}{d^2}, \frac{u_2 H^2}{d^2}, \frac{u_3 H^3}{d^2}, \cdots, \frac{u_n H^n}{d^2}\right).$$

We use this to count polynomials for cubefull d with $H^2 < d < H^3$. As $d < H^3$ and the decay of $\widehat{\phi}$, these sums essentially only have $u_i = 0$ for $i \geq 6$. Recall that the support of $\widehat{\phi}$ has an "arithmetic progression" property — implying that the next couple of coefficients are almost zero. Carrying this out fully shows that we only need to consider when $u_1, u_2 \neq 0$.

Thank you very much.

Please note that these slides (and references for the cited works) are (or will soon be) available on my website (davidlowryduda.com).

References i

- Theresa C. Anderson, Ayla Gafni, Kevin Hughes, Robert J. Lemke Oliver, David Lowry-Duda, Frank Thorne, Jiuya Wang, and Ruixiang Zhang.
  Improved bounds on number fields of small degree, 2022.

- Theresa C Anderson, Ayla Gafni, Robert J Lemke Oliver, David Lowry-Duda, George Shakan, and Ruixiang Zhang.
  Quantitative hilbert irreducibility and almost prime values of polynomial discriminants.
  Int. Math. Res. Not., 2022.
  To appear. `https://arxiv.org/abs/2107.02914`.

- Manjul Bhargava, Arul Shankar, and Xiaoheng Wang.
  Squarefree values of polynomial discriminants I.
  Inventiones Mathematicae, 2022.
  To appear.

References ii

Robert J. Lemke Oliver and Frank Thorne.
Upper bounds on number fields of given degree and bounded discriminant, 2020.
Preprint available at https://arxiv.org/abs/2005.14110.

Wolfgang M. Schmidt.
Number fields of given degree and bounded discriminant.
Astérisque, 228(4):189–195, 1995.
Columbia University Number Theory Seminar (New York, 1992).