DISCRIMINANT BOUNDS AND SOME RELATED TOPICS

FRANK THORNE

Abstract. These notes give a loose overview of Odlyzko's survey [3] of discriminant bounds, along with some additional things I learned from poking into a couple of the references which interested me. Additionally, I list a lot of questions that occur to me, about which I haven't thought about too much.

1. Introduction

Start with a number field K of degree $n = r_1 + 2r_2$, where r_1, r_2 are the number of real/complex embeddings. Let $D = D_K$ denote the absolute value of the discriminant of K. (The sign is $(-1)^{r_2}$.) We are interested in estimates, and in particular, in lower bounds, for the discriminant D.

1.1. **Explicit formulas and stuff.**

The Dedekind zeta function $\zeta_K(s)$ satisfies a functional equation as follows: Let

$$\xi_K(s) := \zeta_K(s)\left(\frac{|D|}{2^{2r_2}\pi^n}\right)^{s/2}\Gamma(s/2)^{r_1}\Gamma(s)^{r_2}.$$

Then

$$\xi_K(s) = \xi_K(1-s).$$

Remark. Different-looking versions of this formula can be found; recall for example Legendre's duplication formula

$$\Gamma(s)\Gamma(s+1/2) = \frac{2\sqrt{\pi}}{2^{2s}}\Gamma(2s).$$

Also, the formula in Neukirch appears to differ by a factor of 2^{r_2}. As this does not depend on s, it does not affect the truth of the functional equation. (But it is still somehow annoying. Which one is "correct"?)

Proposition 1.1. *The (absolute value of the) discriminant D satisfies the following explicit formula for each value of s:*

$$\log D = r_1\left(\log\pi - \frac{\Gamma'}{\Gamma}(s/2)\right) + 2r_2\left(\log(2\pi) - \frac{\Gamma'}{\Gamma}(s)\right) - \frac{2}{s} - \frac{2}{s-1} + 2\sum_\rho{}' \frac{1}{s-\rho} - 2\frac{\zeta_K'}{\zeta_K}(s). \tag{1.1}$$

Proof. Let

$$f(s) := s(s-1)\xi_K(s),$$

so that $f(s) = f(1-s)$, and $f(s)$ is entire. The proof consists of writing down two expressions for $\frac{\zeta'}{\zeta}$. The first is obtained by logarithmically differentiating the formula defining $f(s)$. To obtain the second, we recall that $f(s)$, being an entire function of order 1 (not proved in this note), must have a Hadamard product

$$f(s) = e^{A+Bs}\prod_\rho\left(1-\frac{s}{\rho}\right)e^{s/\rho}.$$

2000 *Mathematics Subject Classification.* 11N25, 11N36.

Logarithmically differentiating we obtain that

$$\frac{f'(s)}{f(s)} = B + \sum_{\rho} \left(\frac{1}{\rho} + \frac{1}{s - \rho} \right).$$

Similarly,

$$\frac{-f'(1-s)}{f(1-s)} = B + \sum_{\rho} \left(\frac{1}{\rho} + \frac{1}{1 - \rho - s} \right).$$

But if ρ is a zero of $f(s)$ then so is $1 - \rho$. So this simplifies to

$$\frac{-f'(1-s)}{f(1-s)} = B + \sum_{\rho} \left(\frac{1}{\rho} - \frac{1}{s - \rho} \right).$$

Now recall that $f(s) = f(1 - s)$ and subtract the second equation from the first. We obtain

$$\frac{f'(s)}{f(s)} = \sum_{\rho}{}' \frac{1}{s - \rho},$$

which is delightfully simple! In particular, the constant B went away.

Remark. Here we take the zeroes in pairs, to make sure everything converges nicely.

Now we equate these two expressions, and we easily obtain the formula claimed. □

Question 1. *I seem to recall other, similar formulas – although some of these may be the result of (ahem!) my mistakes. Are there other formulas which occur and are interesting?*

1.2. **Discriminant bounds.** This formula can be easily used to bound discriminants from below. Let s be any real number > 1. Then

$$\frac{\zeta_K'}{\zeta_K}(s) = \sum_{\mathfrak{p}} \sum_{m \geq 1} \log(\mathbb{N}\mathfrak{p})(\mathbb{N}\mathfrak{p})^{-ms},$$

which is strictly positive, and the sum over zeroes is positive as well (as they occur in complex conjugate pairs) so we obtain the formula

$$\log D \geq r_1(\log \pi - \frac{\Gamma'}{\Gamma}(s-2)) + 2r_2(\log(2\pi) - \frac{\Gamma'}{\Gamma}(s)) - \frac{2}{s} - \frac{2}{s-1}.$$

By taking $s = 1 + n^{-1/2}$ for example we obtain the bound

$$D \geq (4\pi e^{\gamma})^{r_1} (2\pi e^{\gamma})^{r_2} e^{o(n)}.$$

We can also easily obtain bounds which are completely explicit.

Remark. Odlyzko refers to a paper of Serre (in French, unfortunately) which improves on the methods described here and also is (apparently) quite elegant.

1.3. **Why the discriminant?** One interesting question is: Why do we get a formula for the discriminant? How is it that it appears in the functional equation?

Here is a brief summary of the answer. We refer to Neukirch's book [2] for the proof. The idea essentially is that we convert the sum over norms of ideals into a sum first over ideal classes. We choose a representative ideal $\mathfrak{a}$ from each class, and then sum over the elements of this ideal. By adding this up in the appropriate way, we get the Dedekind zeta function. We then see that the Dedekind zeta function is a Mellin tranform of a theta function associated to the ideal.

Anyway, in this calculation the volume of the ideal $\mathfrak{a}$ is relevant, and this volume is given by $\mathbb{N}\mathfrak{a}\sqrt{D_K}$. Hence the discriminant.

Question 2. *What types of formulas do you get for other types of L-functions? Elliptic curves, modular forms, Artin L-functions, automorphic representations, you name it. This formula was proved by writing down a functional equation for the L-function and doing some elementary manipulation.*

2. Lower bounds for discriminants

In this section of Odlyzko's paper, he states the latest bounds for discriminants obtained by use of "explicit formulas of prime number theory".

He gives an explicit formula for the discriminant, which is the following. Consider a differentiable even function $F : \mathbb{R} \to \mathbb{R}$, with $F(0) = 1$, such that

$$|F(x)|, |F'(x)| \leq ce^{-(1/2+\epsilon)|x|}$$

as $|x| \to \infty$. Define

$$\Phi(s) = \int_{-\infty}^{\infty} F(x)e^{(s-1/2)x}dx.$$

The explicit formula for the discriminant is then the following:

$$\log D = \frac{r_1\pi}{2} + n(C + \log(8\pi)) - n\int_0^{\infty} \frac{1 - F(x)}{2\sinh(x/2)}dx - r_1\int_0^{\infty} \frac{1 - F(x)}{2\cosh(x/2)}dx$$
$$-4\int_0^{\infty} F(x)\cosh(x/2)dx + \sum_{\rho}{}' \Phi(\rho) + 2\sum_{\mathfrak{p}}\sum_{m\geq 1} \frac{\log \mathbb{N}\mathfrak{p}}{(\mathbb{N}\mathfrak{p})^{m/2}}F(m\log \mathbb{N}\mathfrak{p}).$$

The principle of the proof (based on a cursory reading of Poitou's paper *Minorations de discriminants*) appears to be that one considers the contour integral

$$\int \Phi(s)d(\log \xi(s)),$$

where $\xi(s)$ is the completed zeta function. One takes the vertical contours at $1 + \alpha$ and $-\alpha$, so that the functional equation applies.

We evaluate on the one hand as a sum of residues, and transform on the other into

$$\frac{1}{2\pi i}\int_{1+\alpha-iT}^{1+\alpha+iT} \frac{\xi'}{\xi}(s)[\Phi(s) + \Phi(1-s)]ds.$$

One splits ξ'/ξ up into its usual parts. The part involving ζ'/ζ gives the sum over prime ideals (although it appears we are evaluating at $s = 1/2$... I'm confused how). The part involving the gamma factors is holomorphic, and so can be translated to the 1/2-line.

We thus obtain formulas like

$$\frac{-1}{2\pi}\int_{-\infty}^{\infty} \Re\frac{\Gamma'}{\Gamma}(\frac{1}{2} + it)\Phi(\frac{1}{2} + it);$$

this is the contribution for each complex place and we get something similar for the real places. An application of Plancherel's formula and a little bit of analysis leads to the curious-looking integrals involving sinh and cosh which you see above.

[As I said before adding the above:] What is interesting about the formula is that there is a sum over both all the zeroes of the zeta function as well as over all the prime ideals. They are weighted against certain kernels: The sum over primes is weighted by a function F which is differentiable and decays nicely at infinity, and the sum over zeroes is weighted by a function Φ, which looks sort of like a Fourier or Mellin transform of F (but which is not exactly either).

We will give a vague account of what Odlyzko says in Section 2 (not that he is all that specific).

The best way to use this formula seems to involve knowing a lot about zeroes and prime ideals. But if you don't, you can simply choose F so that the contributions of prime ideals and zeroes are all negative. The construction of a good F seems a bit complicated (Odlyzko does not bother to describe it). But, you get good bounds for the discriminant. You can also get bounds that are nearly as good with less careful choices of F.

Odlyzko states that no choices can give a better main term on these bounds, but asks which functions give the best error terms.

There are applications of discriminant bounds to estimate class numbers. Although Odlyzko does not describe how this is done, he provides some references. We will digress into Stark's paper [4] and describe one of these references:

2.1. **Stark's application.** Stark starts with the following

Proposition 2.1. *Suppose that $\zeta_K(s)$ does not have an exceptional zero, i.e., $\zeta_K(s) \neq 0$ for $1 - (4\log|D|)^{-1} < s < 1$. Then*

$$hR > c_2^{-n}(1 - s_0)|D|^{1/2},$$

where $s_0 = 1 - (4\log|D|)^{-1}$.

I admit to being a bit confused by the proof. But the basic idea is that

$$\xi(s) = \frac{2^{r_1}Rh}{\omega s(s-1)} + \cdots,$$

where the dots refer to a sum of certain integrals of certain theta functions. This sum is holomorphic, so that this formula gives us the residue at $s = 1$. Furthermore, for real s, the dots are positive.

Now it can be shown that $\xi(s_0)$ is negative, and this implies a lower bound for hR as above.

Now suppose we do not assume the nonexistence of the exceptional zero. The **Brauer-Siegel Theorem** allows us to get around this. As Stark explains, the main idea of the proof is to make the exceptional zeroes of two zeta functions contradict each other by showing that they are both zeroes of the composite field. The upshot is that we obtain an unconditional result

$$HR > c_3(\epsilon)^{-1}|D|^{1/2-\epsilon}.$$

Unfortunately the result is ineffective, as c_3 depends on a hypothetical counterexample to the conjecture.

We also have the "boring half" of the theorem; namely,

$$HR < c_3(\epsilon)|D|^{1/2+\epsilon}.$$

Stark put these two halves together in the following interesting manner: Suppose that we have a totally complex quadratic extension of a totally real number field. Then it can be shown that the regulators of K and k are 'essentially' the same. (The units of k form a subgroup of finite index in K, which can easily be estimated.) We obtain that

$$h(K)/h(k) > c_5(\epsilon)^{-1}|D_K|^{1/2-\epsilon}/|D_k|^{1/2+\epsilon}.$$

Now $|D_K| = D_l^2 f$, where f is an integer (a fact we will not attempt to justify here), and so this implies that

$$h(K) > c_5(\epsilon)^{-1}|D_k|^{1/2-3\epsilon}f^{1/2-\epsilon}h(k).$$

Remark. In Stark's paper the latter $h(k)$ does not appear. Either he has made a mistake, or I have, or he is quietly changing his constant to allow it to depend on k.

Now as K runs through all totally complex quadratic extensions of k, we will have $f \to \infty$, (this is not justified here) and thus we conclude that $h(K) \to \infty$. It is believed that there are infinitely many fields of class number 1, so this shows a way in which they cannot hide. I am omitting some stuff about the Brauer-Siegel theorem... ....) Now if k is fixed and K runs through all quadratic totally complex extensions, we conclude that $h(K) \to \infty$.

Question 3. *Are there applications to real quadratic fields? That seems like an interesting question, and one that has not been analyzed very much.*

There are some applications to arithmetic geometry, with references in Odlyzko's paper.

2.2. **Minimal discriminants.** One interesting question is:

Question 4. *What are the minimal discriminants of number fields of various degrees?*

If K is a number field of degree n, we define the *root discriminant* rd_K of K by

$$rd_K = D_K^{1/n}.$$

The root discriminant is related to the Hilbert class field, as follows: Suppose that a field K has class number h, and its Hilbert class field (i.e. the maximal unramified abelian extension) is L. (Recall that this implies that $[L : K] = h$.) Then, $rd_L = rd_K$. If lower bounds on discriminants imply that $rd_L > rd_K$ for all extensions L of K, then $h(K) = 1$.

For a long time it was believed that if d_n is the minimal root discriminant of a number field of degree n, then $d_n \to \infty$ as $n \to \infty$. This would imply that all Hilbert class field towers terminate, so that all number fields could be embedded in fields of class number one. However, Golod and Shafarevich proved that infinite Hilbert class field towers exist. This has been made more explicit by Martinet.

But still, one naturally asks: What do the values d_n look like as $n \to \infty$? For example, is d_p bounded as p ranges over the primes?

2.3. **Polynomials.** Here is another question. Serre was interested in it, so it must be good. Let M_n denote the smallest absolute value of the discriminant of an irreducible monic polynomial with integral coefficients and degree n.

Question 5. *Is there an infinite subset S of positive integers so that $M_n^{1/n}$ is bounded for $n \in S$?*

We recall the relationship between discriminants of polynomials and discriminants of number fields. Suppose that K is a number field with a *power basis*; i.e., an integral basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. Then the discriminant of K equals the discriminant of the minimal polynomial of α.

Question 6. *What is the relationship between these two discriminants in general? Suppose you have a number field K of degree n. Then $K = \mathbb{Q}(\alpha)$ for a primitive element α of degree n. But O_K is not necessarily generated by powers of α.*

This question is sort of vague and the answer may be well known to algebraists.

3. Elkies' GRH bound for discriminants

To be (maybe) added.

4. Prime ideals of small norms

Suppose something is known about the prime ideals of small norms. For example, suppose there are no primes of norm 2 or 3. Then can we prove more?

In the Section 2 discussion above, recall our function F. These decrease very rapidly as $x \to \infty$ – at least they do if we are to get optimal results without knowing very much. But previously all we used was that the contributions of both zeroes and poles were nonnegative. Can we put some meat on the bones?

Odlyzko describes the following example: For $w \in [1, 2]$, take

$$F(x) = \frac{1}{\cosh(\omega - 1/2)x}.$$

Then (as I confess I didn't bother to verify) $\Re\Phi(s) \geq 0$ for $0 \leq Re(s) \leq 1$, and

$$\Phi(0) = 2\int_0^x F(x)\cos(x/2)dx = \frac{1}{\omega - 1} + O(\omega - 1).$$

However,

$$2\sum_{\mathfrak{p}}\sum_{m\geq 1}\frac{\log \mathbb{N}\mathfrak{p}}{\mathbb{N}\mathfrak{p}^{m/2}}F(m\log \mathbb{N}\mathfrak{p}) \geq -\frac{8}{3}\frac{\zeta_K'}{\zeta_K}(\omega).$$

To show this last equation, one checks term by term, and shows for each prime $\mathfrak{p}$ (or really, for each norm of such a prime) that

$$(\mathbb{N}\mathfrak{p})^{m(\omega-1/2)}\frac{2}{(\mathbb{N}\mathfrak{p})^{m(\omega-1/2)} + (\mathbb{N}\mathfrak{p})^{-m(\omega-1/2)}} \geq \frac{4}{3}.$$

For $\mathbb{N}\mathfrak{p} = 2$ you get strict equality, and for higher norms you get an inequality. If there are no primes of norm 3 you can do better, and so on, but of course you can't get to -4. In any case, one obtains the formula

$$\log D > r_1 \log 60.7 + 2r_2 \log 22.35 - \frac{8}{3}\frac{\zeta_K'}{\zeta_K}(\omega) - \frac{2}{\omega - 1},$$

for $\omega \in (1, 1+\delta)$ for some $\delta > 0$ and $n \gg 1$.

As Odlyzko states, one can devise other kernels $F(x)$ that will emphasize the contributions of particular ideals.

Question 7 (Not stated by Odlyzko – but implicit!). *Are there number fields where we know enough about the ideals to do anything useful in this regard?*

5. Minkowski constants and regulators

Suppose that $L_1(x), \dots, L_n(x)$ are linear forms in the variables $x_1, \cdots, x_n$, where we write $x = (x_1, x_2, \cdots, x_n)$. Then "geometry of numbers" bounds state that there are integer values of the x_i such that the product $\prod L_j(x)$ is small.

Question 8. *How would you prove such bounds?*

We can use these bounds to prove that each ideal class of K contains an ideal of small norm, say with

$$N\mathfrak{a} \leq (C_1 - o(1))^{-r_1/2}(C_2 - o(1))^{-r_2}D^{1/2}.$$

Presumably, one starts with the usual proof of the finiteness of the class number (... which I should read again...) and makes some improvements somewhere.

We can use the trivial bound $\mathbb{N}\mathfrak{a} \geq 1$ to prove a bound of the form

$$D \geq (C_1 - o(1))^{r_1}(C_2 - o(1))^{2r_2},$$

which is of the same shape as before. (Presumably we got values of C_1 and C_2 from whatever geometry of numbers proof we came up with.) But we have lost some information here.

Question 9 (Odlyzko's)**.** *What are the best constants that can be used above?*

Question 10 (mine)**.** *What are some interesting applications below proving lower bounds for the discriminant?*

There are also some questions of proving lower bounds for regulators of number fields, with some references – we won't go into that here.

6. Low zeroes of Dedekind zeta functions

Recall all of our explicit formulas. They are *equalities* for the discriminant. So, when D is larger than the bound, that is due either due to the contribution of prime ideals or to the contribution of zeroes. Our kernels are such that the contribution of prime ideals of large norm is negligible, and the contribution of zeroes far from the real axis are negligible. Thus, high discriminants point to primes of small norm, to low-lying zeroes, or to both.

Question 11. *How easy is it to compute low-lying zeroes of Dedekind zeta functions? Odlyzko says that there is a nice method, but it has not been implemented yet. However, his paper was written twenty years ago.*

Odlyzko poses the following question:

Question 12. *What are the relative contributions of prime ideals and zeroes to the explicit formula for* **minimal discriminants** *(i.e., for fixed degree n, and possibly for fixed r_1 and r_2, the smallest discriminant of any field with that degree).*

Aside: this suggests the following to me:

Question 13. *For fixed n, r_1, r_2, how many number fields of discriminant $< X$ are there?*

Quadratic fields are known, and cubic fields are given to us by Davenport-Heilbronn.

Back to Odlyzko's question, the numerical data does not seem to suggest anything all that interesting. In particular, it does not appear that either the zeroes or the ideals dominate, although this depends on our choice of kernel.

Odlyzko suggests another question:

Question 14. *Do the zeroes of $\zeta_K(s)$ in the critical strip approach the real axis as $n \to \infty$? If so, how fast do they do so, any how many of them are there.*

If we let $D \to \infty$ for fixed n, then we know there will be zeroes arbitrarily close to the real axis. (Consider trying to find a proof in Iwaniec-Kowalski?) Also, Odlyzko did prove that $\zeta_K(s)$ has a zero on the critical line at height $O((\log n)^{-1})$, but only conditionally on GRH. Unconditionally, he only proved that there is a zero at height $\leq 0.54 + o(1)$.

Remark. An attempt to find proofs of these statements in the literature was unsuccessful. In particular, Odlyzko references a preprint which does not seem to have appeared.

Question 15. *Can you at least prove something unconditional for some sort of families, for "almost all", etc.?*

Question 16. *What about, say, for modular L-functions? Are there interesting applications?*

Question 17. *What about function fields and low-lying zeroes? I believe I've read something about this, but I forget what. Naturally, the zeta functions in function fields assume a simpler form. It still seems very interesting to look at the distribution of the zeroes.*

6.1. **Katz-Sarnak, monodromy, and other such fun.** Along these lines, we should certainly mention the Katz-Sarnak results. Assume GRH. Let ϕ be a nice test function (i.e., one with rapid decay) and consider the low-zeroes sum

$$D(f,\phi) := \sum_{\gamma_f} \phi\left(\gamma_f \frac{\log c_f}{2\pi}\right).$$

Here γ_f runs over the ordinates of zeroes counted with multiplicity. The $\log c_f$ factor is for normalization purposes (here c_f is the conductor of the L-function); we have

$$N(T,f) \sim \frac{dT}{2\pi} \log c_f T,$$

so that the expected behavior of $D(f,\phi)$ should be the same within a family of L-functions of the same degree.

Let $\mathcal{F}$ be a nice family of L-functions, and let $\mathcal{F}(Q)$ be the subset with conductor Q. We have the following (vague) conjecture.

Conjecture 1. *If $\mathcal{F}$ is a "complete" family (in a certain spectral sense), then*

$$\frac{1}{\mathcal{F}(Q)} \sum_{f \in \mathcal{F}(q)} D(f,\phi) \sim \int_{\mathbb{R}} \phi(x) W(\mathcal{F})(x) dx,$$

where $W(\mathcal{F})(x)$ is a density function characterized by $\mathcal{F}$.

What Katz and Sarnak determined was that this density function is determined by a certain monodromy group associated to $\mathcal{F}$. For example, consider the family of Dirichlet L-functions for real characters χ. Then,

$$W(x) = W_{sp}(x) = 1 - \frac{\sin 2\pi x}{2\pi x}.$$

If one starts with an elliptic curve L-function, and twists by real characters, one expects

$$W(x) = W^{+}(x) = 1 + \frac{sin 2\pi x}{2\pi x}.$$

There are further examples; see Section 25.4 of Iwaniec and Kowalski's book for an introduction and references.

We mention additionally that part of what makes these conjectures so convincing is their analogues for function fields. There the zeroes are eigenvalues of the Frobenius operator, so that there is a geometric explanation for these phenomena.

Question 18. *Perhaps this is not as interesting, but can one do some sort of brute force argument along the lines of Odlyzko for individual L-functions over function fields?*

References

[1] J. Lagarias and A. Odlyzko, *Effective versions of the Chebotarev density theorem*, some obscure conference proceedings, unfortunately not available online.

[2] J. Neukirch, *Algebraic number theory*.

[3] A. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators, and zeros for zeta functions: a survey of recent results*, to be found on his website.

[4] H. Stark, *The analytic theory of algebraic numbers*.

Department of Mathematics, Stanford University

E-mail address: fthorne@math.stanford.edu