Math 229: Introduction to Analytic Number Theory

How small can $|\mathrm{disc}(K)|$ be for a number field K of degree $n = r_1 + 2r_2$?

Let K be a number field of degree $n = r_1 + 2r_2$, where as usual r_1 and r_2 are respectively the numbers of real embeddings and conjugate complex embeddings of K. Let O_K be the ring of algebraic integers of K, and $D_K = \mathrm{disc}(K/\mathbf{Q})$ the discriminant. Minkowski proved that every ideal class of K contains some ideal $J \subseteq O_K$ of norm at most $(n!/n^n)(4/\pi)^{r_2}|D_K|^{1/2}$. (See for instance [Marcus 1977].) In particular, the principal ideal class contains such a J (which might as well be taken to be O_K itself), and since the norm of J is at least 1 we recover the *Minkowski bound*

$$|D_K| \geq \left(\frac{\pi}{4}\right)^{2r_2} \left(\frac{n^n}{n!}\right)^2. \tag{1}$$

In particular, it readily follows that $|D_K| > 1$ once $n > 1$ (that is, except for $K = \mathbf{Q}$); that is, $\mathbf{Q}$ *has no nontrivial unramified extension.* This is a key ingredient of the Kronecker-Weber theorem, which asserts that any finite extension of $\mathbf{Q}$ with abelian Galois group is contained in a cyclotomic extension $\mathbf{Q}(e^{2\pi i/n})$.

Asymptotically as $n \to \infty$, Minkowski's bound is

$$\log|D_K| \geq (2 - o(1))n - 2\log(4/\pi)r_2. \tag{2}$$

That is, we have the lower bound $(\pi/4)^{2r_2/n}e^2 - o(1)$ on the "root-discriminant" $|D_K|^{1/n}$. (Note for future reference the numerical values: $(\pi/4)^{2r_2/n}e^2$ is approximately $(7.389)^{r_1/n}(5.803)^{2r_2/n}$.) It is known that the root-discriminant is invariant under unramified extensions; for instance (1) also implies that some other number fields — such as the quadratic fields $\mathbf{Q}(e^{2\pi i/3})$, $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{5})$ whose discriminants $-3, -4, 5$ have the smallest absolute values — have no nontrivial unramified extension. Subsequent work extended Minkowski's "geometry of numbers" to show $\log|D_K|$ is bounded below by larger linear combinations of r_1, r_2.

In the other direction, Golod and Šafarevič proved that quadratic number fields K_0 whose discriminants have many prime factors have an infinite "class field tower", and thus unramified extensions K with $[K : K_0] \to \infty$. Such K all have root-discriminant $|D_{K_0}|^{1/2}$. There is thus an upper limit to improvements on the constants in (2). One survey of such constructions and the resulting upper limits is [Schoof 1986].

Much less is known here than for the analogous question on curves C of high genus with many points over a fixed finite field k. (See the Remarks below.) The best lower bounds for all but the smallest few n are now obtained by a method independent of Minkowski's approach, and similar to the techniques that yield upper bounds on $\#C(k)$. The method, attributed to Stark [1974, 1975] by Odlyzko [1991], uses the Euler and Hadamard products for the zeta function ζ_K to transform the functional equation for ζ_K into a formula for $\log|D_K|$ in terms of r_1, r_2, and the nontrivial zeros of ζ_K. In a series of papers starting from [Odlyzko 1975], the bounds were progressively improved until reaching their present form:

Theorem. *Let K be a number field of degree $n = r_1 + 2r_2$. Then*

$$\log |D_K| > (\log 4\pi + \boldsymbol{\gamma} - o(1))n + r_1 \tag{3}$$

as $n \to \infty$, where $\boldsymbol{\gamma} = -\Gamma'(1) = .577\ldots$ is Euler's constant. If moreover ζ_K satisfies the Generalized Riemann Hypothesis then

$$\log |D_K| > (\log 8\pi + \boldsymbol{\gamma} - o(1))n + (\pi/2)r_1 \tag{4}$$

as $n \to \infty$.

Numerically, the root-discriminant of K is asymptotically bounded below by $(60.8)^{r_1/n}(22.38)^{2r_2/n}$, and by $(215.3)^{r_1/n}(44.7)^{2r_2/n}$ under the GRH. For many applications one needs also explicit estimates on the $o(1)$ terms for specific values of (r_1, r_2). Odlyzko carried out extensive numerical computations to obtain good lower bounds for many (r_1, r_2). See [Odlyzko 1991] for a survey of the methods used and some of the applications, which include the theorem that each of the nine imaginary quadratic fields of class number 1 has no nontrivial unramified extensions. (NB the last of these fields has root-discriminant $\sqrt{163} < 13$.)

We present only a simple proof of the asymptotic estimate under GRH, making no attempt to optimize the $o(1)$ error. The same approach yields the unconditional bound (3); see the Exercises.

We begin by obtaining Artin's formula for $|D_K|$:

Proposition. *For all real $s > 1$ we have*

$$\begin{aligned}\log |D_K| \;=\; & r_1\Big(\log \pi - \frac{\Gamma'}{\Gamma}(s/2)\Big) + 2r_2\Big(\log 2\pi - \frac{\Gamma'}{\Gamma}(s)\Big) \\ & - \frac{2}{s-1} - \frac{2}{s} - 2\frac{\zeta_K'}{\zeta_K}(s) + \; 2\sum_\rho \operatorname{Re}\frac{1}{s-\rho},\end{aligned} \tag{5}$$

where ρ runs over the nontrivial zeros of $\zeta_K(s)$ counted with multiplicity.

Proof: Recall that the functional equation for ζ_K may be written in the form

$$\xi_K(s) := \Gamma(s/2)^{r_1}\Gamma(s)^{r_2}(4^{-r_2}\pi^{-n}|D_K|)^{s/2}\zeta_K(s) = \xi_K(1-s), \tag{6}$$

and that $(s^2 - s)\xi_K(s)$ is an entire function of s of order 1. Translation by 1/2 yields the entire function $(s^2 - \frac{1}{4})\xi_K(s + \frac{1}{2})$ symmetric under the involution $s \mapsto -s$. The logarithmic derivative of the Hadamard product for this function yields the partial-fraction decomposition

$$\frac{\xi_K'(s)}{\xi_K(s)} = B - \frac{1}{s} + \frac{1}{1-s} + \frac{m}{s-\frac{1}{2}} + \sum_\rho \left(\frac{1}{s-\rho} + \frac{1}{\rho - \frac{1}{2}}\right). \tag{7}$$

Here m is the multiplicity of the zero, if any, of $\zeta_K(s)$ at $s = 1/2$; and ρ runs over the nontrivial zeros of $\zeta_K(s)$ counted with multiplicity, excluding 1/2. Since (7) is an odd function of $s - 1/2$, the constant B must vanish. We can now take the logarithmic derivative of (6) and solve for $|D_K|$. Averaging the ρ and $1 - \rho$ terms, we may replace the summand $(s - \rho)^{-1} + (\rho - \frac{1}{2})^{-1}$ by

$$\frac{1}{2}\Big(\frac{1}{s-\rho} + \frac{1}{s-(1-\rho)}\Big).$$

Having thus eliminated $(\rho - \frac{1}{2})^{-1}$, we recover (5) as follows. For real s, we know $\zeta_K'(s)/\zeta_K(s) \in \mathbf{R}$, so we may replace $((s-\rho)^{-1} + (s-1+\rho)^{-1})/2$ by its real part. Since each ρ has real part in $(0,1)$, we have $\mathrm{Re}(1/(s-\rho)) \ll \mathrm{Im}(\rho)^{-2}$ as $|\rho| \to \infty$, so $\sum_\rho \mathrm{Re}(1/(s-\rho))$ converges absolutely. We may therefore rearrange the sum, including the contribution of a possible zero at 1/2, to obtain (5). $\square$

For large n we already improve on the Minkowski bound using (5). Fix $s > 1$; then each of the terms $\mathrm{Re}(1/(s-\rho))$ is positive, as is $-2\zeta_K'(s)/\zeta_K(s)$ by the Euler product, while the negative terms $-2/(s-1) - 2/s$ are constants. Hence

$$\log|D_K| > r_1\Big(\log\pi - \frac{\Gamma'}{\Gamma}(s/2)\Big) + 2r_2\Big(\log 2\pi - \frac{\Gamma'}{\Gamma}(s)\Big) - O(1). \tag{8}$$

Now take s arbitrarily close to 1; then $-(\Gamma'/\Gamma)(s/2)$ and $-(\Gamma'/\Gamma)(s)$ approach $-(\Gamma'/\Gamma)(1/2)$ and $-(\Gamma'/\Gamma)(1)$, which equal $\boldsymbol{\gamma} + \log 4$ and $\boldsymbol{\gamma}$ respectively, and we deduce

$$\log|D_K| > (\log 2\pi + \boldsymbol{\gamma} - o(1))n + (\log 2)r_1 \tag{9}$$

which yields an asymptotic lower bound $(22.38)^{r_1/n}(11.19)^{2r_2/n}$ on the root-discriminant.

The *Proof* of (4) improves on this further. Start by using the Euler product to show that not only $-\zeta_K'/\zeta_K$ but also all its derivatives of even order with respect to s are positive for $s > 1$, while the derivatives of odd order are negative. Thus by differentiating (5) m times $(m = 0, 1, 2, \ldots)$ we find

$$\begin{aligned}\delta_m \log|D_K| \;&>\; (-1)^m\Big[r_1\frac{d^m}{ds^m}\Big(\log\pi - \frac{\Gamma'}{\Gamma}(s/2)\Big) + 2r_2\frac{d^m}{ds^m}\Big(\log 2\pi - \frac{\Gamma'}{\Gamma}(s)\Big)\Big] \\ &\quad + m!\Big(2\sum_\rho \mathrm{Re}\,\frac{1}{(s-\rho)^{m+1}} \;-\; \frac{2}{(s-1)^{m1}} - \frac{2}{s^{m+1}}\Big).\end{aligned} \tag{10}$$

(Here δ_m is a form of Kronecker's delta, which equals 1 for $m = 0$ and zero otherwise.)

Our idea is now that for fixed $s > 1$ and large n the term in $(s-1)^{-(m+1)}$ is negligible, and so by dividing the rest of (10) by $2^m m!$ and summing over m we obtain (5) with s replaced by $s - 1/2$ (Taylor expansion about s). Since $\mathrm{Re}(1/(s - \frac{1}{2} - \rho))$ is still positive, we then find by bringing s arbitrarily close to 1 that

$$\log|D_K| > r_1(\log\pi - \frac{\Gamma'}{\Gamma}(1/4)) + 2r_2(\log 2\pi - \frac{\Gamma'}{\Gamma}(1/2)) - o(n),$$

and thus obtain our Theorem from the known special values

$$\frac{\Gamma'}{\Gamma}(1/2) = -\log 4 - \boldsymbol{\gamma}, \quad \frac{\Gamma'}{\Gamma}(1/4) = -\log 8 - \pi/2 - \boldsymbol{\gamma}. \tag{11}$$

To make this rigorous, we argue as follows. For any small $\epsilon > 0$, take $s_0 = 1+\epsilon$, and pick an integer M so large that

> (i) the values at $s = s_0 - 1/2$ of the M-th partial sums of the Taylor expansions of $(\Gamma'/\Gamma)(s)$ and $(\Gamma'/\Gamma)(s/2)$ about $s = s_0$ are within ϵ of $(\Gamma'/\Gamma)(s_0 - \frac{1}{2})$ and $(\Gamma'/\Gamma)(s_0/2 - \frac{1}{4})$ respectively;
>
> (ii) the value at $s = s_0 - 1/2$ of the M-th partial sum of the Taylor expansion of $\mathrm{Re}(1/(s-\frac{1}{2}-\rho))$ about $s = s_0$ is positive for all complex numbers ρ of real part $1/2$.

Condition (i) holds for large enough M because $(\Gamma'/\Gamma)(s)$ and $(\Gamma'/\Gamma)(s/2)$ are both analytic functions of s in a circle of radius $1 > 1/2$ about s_0. To verify that (ii) also holds as $M \to \infty$, let[1] $\rho = 1/2 + it$, and note that $\mathrm{Re}(1/(s - \frac{1}{2} - \rho)) = \mathrm{Re}(1/(s - it)) = \epsilon/(\epsilon^2 + \mathrm{Im}(\rho)^2)$, and the value of the M-th partial sum of the Taylor expansion differs from this by

$$\mathrm{Re}\, \frac{1}{[1 + 2(\epsilon - it)]^M (\epsilon + it)} \ll (1 + \epsilon^2 + t^2)^{-M/2}.$$

The positive $\epsilon/(\epsilon^2 + t^2)$ clearly dominates the error $(1 + \epsilon^2 + t^2)^{-M/2}$ uniformly in t once M is sufficiently large.

Now divide (10) by $2^m m!$, sum from $m = 0$ to $M - 1$, and set $s = s_0$ to obtain

$$\log |D_K| > r_1 \Big(\log \pi - \frac{\Gamma'}{\Gamma}(s_0/2 - 1/4) - \epsilon \Big) + 2r_2 \Big(\log 2\pi - \frac{\Gamma'}{\Gamma}(s_0 - 1/2) - \epsilon \Big) + O(1);$$

since ϵ was arbitrarily small and s_0 arbitrarily close to 1, we are done. □□

Remarks

Besides the problem of evaluating limits such as $\liminf_{n\to\infty} \log |D_K|/n$, many other natural questions remain wide open in this context where analogous questions for high-genus curves with many rational points over a finite field have been settled for some time. We list several of these open questions:

- It is not known how to construct class field towers explicitly. Can one construct an explicit infinite sequence of number fields K with bounded root-discriminant?
- When a class field tower over K_0 can be proved infinite, the resulting unramified extensions K have $[K : K_0]$ limited to a very sparse set of positive integers, namely those whose prime factors are contained in a given finite set S. Does there exist $\theta > 0$ an infinite sequence of number fields K with bounded root-discriminant whose degrees cover at least x^θ of the integers $n < x$ as $x \to \infty$?
- More ambitiously: Can there be such a sequence that covers *every* n? Equivalently, is $\limsup_{n\to\infty} \log |D_K|/n$ finite?

[1]The customary $\rho = 1/2 + i\gamma$ may lead to confusion in the presence of Euler's constant $\boldsymbol{\gamma}$.

- In another direction: in a class field tower over a fixed number field, the ratios r_1/n are limited to a small subset of $[0,1] \cap \mathbf{Q}$. Does there exist a finite R such that the number fields K with $|D_K| < R^n$ have ratios r_1/n that form a dense subset of $[0,1]$, or even of an interval of positive length in $[0,1]$?

- The ratio r_1/n can be regarded as a measure of the behavior of the "archimedean place" of $\mathbf{Q}$ in K. Similar questions can be posed concerning the splitting or ramification of a given set of "nonarchimedean places" (rational primes) in K. See also Exercise 4.

Another notable application of the method of Odlyzko et al. is Mestre's lower bound on the conductor of an elliptic curve $E/\mathbf{Q}$ of given rank, assuming GRH as well as the conjecture of Birch and Swinnerton-Dyer for the L-function $L(E,s)$ of the curve. Similar bounds have been obtained for even more complicated L-functions.

Exercises

1. Fill in the missing steps in our proof of (4) by checking the derivation of the formula (5) or $\log|D_K|$ and proving the formulas (11) for the logarithmic derivative of $\Gamma(s)$ at $s = 1/2$ and $s = 1/4$.

2. Show that the Odlyzko bound (4) still holds under the weakened hypothesis that all zeros of $\zeta_K(s)$ are either real or on the critical line $\sigma = 1/2$. (This hypothesis allows also for nontrivial zeros on $(0,1)$.) Can you find a yet weaker hypothesis on the zeros under which (4) remains true?

3. Use the same methods to prove the unconditional lower bound (3).

4. Suppose that the rational prime 2 splits completely in K (whence the Euler product for $\zeta_K(s)$ contains the factor $(1-2^{-s})^{-n}$). Obtain lower bounds on $|D_K|$, both unconditionally and under GRH, that improve on (3,4). Generalize.

References

[Marcus 1977] Marcus, D.A.: *Number Fields.* New York: Springer, 1977.

[Odlyzko 1975] Odlyzko, A.M.: Some analytic estimates of class numbers and discriminants, *Invent. Math.* **29** (1975) #3, 275–286.

[Odlyzko 1991] Odlyzko, A.M.: Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results, *Sém. Th. des Nombres Bordeaux (2)* **2** (1990) #1, 119–141.

[Schoof 1986] Schoof, R.: Infinite class field towers of quadratic fields, *J. reine angew. Math.* **372** (1986), 209–220.

[Stark 1974] Stark, H.M.: Some effective cases of the Brauer-Siegel theorem, *Invent. Math.* **23** (1974), 135–152.

[Stark 1975] Stark, H.M.: The analytic theory of algebraic numbers, *Bull. Amer. Math. Soc.* **81)** (1975), 961–972. *Invent. Math.* **23** (1974), 135–152.