19 The analytic class number formula

In the previous lecture we proved Dirichlet's theorem on primes in arithmetic progressions modulo the claim that the L-function $L(s,\chi)$ is holomorphic and nonvanishing at $s=1$ for all non-principal Dirichlet characters χ. To establish this claim we will prove a more general result that has many other applications.

Recall that the Dedekind zeta function of a number field K is defined by

$$\zeta_K(s) := \sum_{\mathfrak{a}} \mathrm{N}(\mathfrak{a})^{-s} = \prod_{\mathfrak{p}} (1-\mathrm{N}(\mathfrak{p})^{-s})^{-1},$$

where $\mathfrak{a}$ ranges over nonzero ideals of $\mathcal{O}_K$ and $\mathfrak{p}$ ranges over nonzero prime ideals of $\mathcal{O}_K$; as we showed in the previous lecture the sum and product converge absolutely on $\mathrm{Re}(s)>1$.

The following theorem is often attributed to Dirichlet, although he originally proved it only for quadratic fields (this is all he needed to prove his theorem on primes in arithmetic progressions, but we will use it in a stronger form). The formula for the limit in the theorem was proved by Dedekind [2, Supplement XI] (as a limit from the right, without an analytic continuation to a punctured neighborhood of $z=1$), and analytic continuation was proved by Landau [3]. Hecke later showed that, like the Riemann zeta function, the Dedekind zeta function has an analytic continuation to all of $\mathbb{C}$ and satisfies a functional equation [1], but we won't take the time to prove this; see Remark §19.13 for details.

Theorem (Analytic Class Number Formula)**.** *Let K be a number field of degree n. The Dedekind zeta function $\zeta_K(z)$ extends to a meromorphic function on $\mathrm{Re}(z) > 1-\frac{1}{n}$ that is holomorphic except for a simple pole at $z=1$ with residue*

$$\lim_{z\to 1^+}(z-1)\zeta_K(z) = \frac{2^r(2\pi)^s h_K R_K}{w_K |D_K|^{1/2}},$$

where r and s are the number of real and complex places of K, respectively, $h_K := \#\operatorname{cl}\mathcal{O}_K$ is the class number, R_K is the regulator, $w_K := \#\mu_K$ is the number of roots of unity, and $D_K := \operatorname{disc}\mathcal{O}_K$ is the absolute discriminant.

Recall that $|D_K|^{1/2}$ is the covolume of $\mathcal{O}_K$ as a lattice in $K_{\mathbb{R}} := K\otimes_{\mathbb{Q}}\mathbb{R} \simeq \mathbb{R}^r\times\mathbb{C}^s$ (Proposition 14.15), and R_K is the covolume of $\Lambda_K := \mathrm{Log}(\mathcal{O}_K^\times)$ as a lattice in the trace-zero hyperplane $\mathbb{R}_0^{r+s}$ (see Definition 15.16). The residue of $\zeta_K(z)$ at $z=1$ thus reflects both the additive and multiplicative structure of the ring of integers $\mathcal{O}_K$.

Remark 19.1. In practice the class number h_K is usually the most difficult quantity in the analytic class number formula to compute. We can approximate the limit on the LHS to any desired precision using a finite truncation of either the sum or product defining $\zeta_K(s)$. Provided we can compute the other quantities to similar precision, this provides a method for computing (or at least bounding) the class number h_K; this explains the origin of the term "analytic class number formula". You will have an opportunity to explore a computational application of this formula on Problem Set 9.

Example 19.2. For $K=\mathbb{Q}$ we have $n=1$, $r=1$, $s=0$, $h=1$, $w=\#\{\pm1\}=2$, $D=1$, and the regulator R is the covolume of a lattice in a zero-dimensional vector space, equivalently, the determinant of a 0×0 matrix, which is 1. In this case the theorem states that $\zeta_{\mathbb{Q}}(z)=\zeta(z)$ is holomorphic on $\mathrm{Re}\,z > 1-\frac{1}{1}=0$ except for a simple pole at $z=1$ with residue

$$\lim_{z\to 1^+}(z-1)\zeta_{\mathbb{Q}}(z) = \frac{2^1(2\pi)^0\cdot 1\cdot 1}{2\cdot |1|^{1/2}} = 1.$$

19.1 Lipschitz parametrizability

In order to prove the analytic class number formula we need an asymptotic estimate for the number of nonzero $\mathcal{O}_K$-ideals $\mathfrak{a}$ with absolute norm $\mathrm{N}(\mathfrak{a})$ bounded by a parameter $t \in \mathbb{R}_{>0}$ that we will let tend to infinity; this is necessary for us to understand the behavior of $\zeta_K(z) = \sum_{\mathfrak{a}} \mathrm{N}(\mathfrak{a})^{-z}$ as $z \to 1^+$. Our strategy is to count points in $\mathrm{Log}(\mathcal{O}_K \cap K^\times)$ that lie inside a suitably chosen region S of $\mathbb{R}^{r+s}$ that we will than scale by t. In order to bound this count as a function of t we need a condition on S that ensures that the count grows smoothly with t; this requires S to have a "reasonable" shape. A sufficient condition for this is *Lipschitz parametrizability*.

Definition 19.3. Let X and Y be metric spaces. A function $f : X \to Y$ is *Lipschitz continuous* if there exists $c > 0$ such that for all distinct $x_1, x_2 \in X$

$$d(f(x_1), f(x_2)) \le c \cdot d(x_1, x_2).$$

Every Lipschitz continuous function is uniformly continuous, but the converse need not hold. For example, the function $f(x) = \sqrt{x}$ on $[0, 1]$ is uniformly continuous but not Lipschitz continuous, since $|\sqrt{1/n} - 0|/|1/n - 0| = \sqrt{n}$ is unbounded as $1/n \to 0$.

Definition 19.4. A set B in a metric space X is *d-Lipschitz parametrizable* if it is the union of the images of a finite number of Lipschitz continuous functions $f_i \colon [0, 1]^d \to X$.

Before stating our next result, we recall the asymptotic notation

$$f(t) = g(t) + O(h(t)) \qquad (\text{as } t \to a),$$

for real or complex valued functions f, g, h of a real variable t, which means

$$\limsup_{t \to a} \left| \frac{f(t) - g(t)}{h(t)} \right| < \infty.$$

Typically $a = \infty$, and this is assumed if a is not specified.

Lemma 19.5. *Let $S \subseteq \mathbb{R}^n$ be a measurable set whose boundary $\partial S := \overline{S} - S^0$ is $(n-1)$-Lipschitz parametrizable. Then*

$$\#(tS \cap \mathbb{Z}^n) = \mu(S)t^n + O(t^{n-1}),$$

as $t \to \infty$, where μ is the standard Lebesgue measure on $\mathbb{R}^n$.

Proof. It suffices to prove the lemma for positive integers, since $\#(tS \cap \mathbb{Z}^n)$ and $\mu(S)t^n$ are both monotonically increasing functions of t and $\mu(S)(t+1)^n - \mu(S)t^n = O(t^{n-1})$. We can partition $\mathbb{R}^n$ as the disjoint union of half-open cubes of the form

$$C(a_1, \dots, a_n) = \{(x_1, \dots, x_n) \in \mathbb{R}_n : x_i \in [a_i, a_i + 1)\},$$

with $a_1, \dots, a_n \in \mathbb{Z}$. Let $\mathcal{C}$ be the set of all such half-open cubes C. For each $t > 0$ define

$$B_0(t) := \#\{C \in \mathcal{C} : C \subseteq tS\},$$
$$B_1(t) := \#\{C \in \mathcal{C} : C \cap tS \neq \emptyset\}.$$

For every $t > 0$ we have

$$B_0(t) \le \#(tS \cap \mathbb{Z}^n) \le B_1(t).$$

We can bound $B_1(t) - B_0(t)$ by noting that each $C(a_1, \dots, a_n)$ counted by this difference contains a point $(a_1, \dots, a_n) \in \mathbb{Z}^n$ within a distance $\sqrt{n} = O(1)$ of a point in $\partial tS = t\partial S$.

Let $f_1, \dots, f_m$ be Lipschitz functions $[0,1]^{n-1} \to \partial S$ whose images cover ∂S, and let $c_1, \dots c_m$ be constants such that $d(f_i(x_1), f_i(x_2)) \le c_i d(x_1, x_2)$ for all $x_1, x_2 \in [0,1]^{n-1}$. For any $y \in \partial S$, we have $y = f_i(x_1, \dots, x_{n-1})$ for some i, and if we put $r_j = \lfloor t x_j \rfloor \in \mathbb{Z}$ so that $0 \le x_j - r_j/t \le 1/t$, then

$$d(y, f_i(\tfrac{r_1}{t}, \dots, \tfrac{r_{n-1}}{t})) \;\le\; c_i \cdot d\big((x_1, \dots, x_{n-1}), (\tfrac{r_1}{t}, \dots, \tfrac{r_{n-1}}{t})\big) \;<\; c_i\sqrt{n}/t \;\le\; c/t,$$

where $c \coloneqq \sqrt{n} \max_i c_i$. Thus every $y \in \partial S$ lies within a distance c/t of a point in the set

$$\mathcal{P} = \left\{ f_i\left(\tfrac{r_1}{t}, \dots, \tfrac{r_{n-1}}{t}\right) : 1 \le i \le m,\ 0 \le r_1, \dots, r_{n-1} \le t \right\},$$

which has cardinality $m(t+1)^{n-1} = O(t^{n-1})$. It follows that every point of ∂tS is within a distance c of one of the $O(t^{n-1})$ points in $t\mathcal{P}$. The number of integer lattice points within a distance $\sqrt{n}$ of a point in $t\partial S$ is thus also $O(t^{n-1})$, and therefore

$$B_1(t) - B_0(t) = O(t^{n-1}).$$

We now note that $B_0(t) \le \mu(tS) \le B_1(t)$ and $\mu(tS) = t^n \mu(S)$; the lemma follows. □

Corollary 19.6. *Let Λ be a lattice in an $\mathbb{R}$-vector space $V \simeq \mathbb{R}^n$ and let $S \subseteq V$ be a measurable set whose boundary is $(n-1)$-Lipschitz parametrizable. Then*

$$\#(tS \cap \Lambda) = \frac{\mu(S)}{\operatorname{covol}(\Lambda)} t^n + O(t^{n-1}).$$

Proof. The case $\Lambda \subseteq \mathbb{Z}^n$ is given by the lemma; note that the normalization of the Haar measure μ is irrelevant, since we are taking a ratio of volumes which is necessarily preserved under the isomorphism of topological vector spaces $V \simeq \mathbb{R}^n$. We now note that if the corollary holds for $s\Lambda$, for some $s > 0$, then it also holds for Λ, since $tS \cap s\Lambda = (t/s)S \cap \Lambda$. For any lattice Λ, we can choose $s > 0$ so that $s\Lambda$ is arbitrarily close to an integer lattice (for example, take s to be the LCM of all denominators appearing in rational approximations of the coordinates of a basis for Λ), which is necessarily a finite index subgroup of $\mathbb{Z}^n$. The corollary follows. □

Remark 19.7. Recall that $\operatorname{covol}(\Lambda) = \mu(F)$ for any fundamental region F for Λ, so the ratio $\mu(S)/\operatorname{covol}(\Lambda) = \mu(S)/\mu(F)$ in Corollary 19.6 does not depend on the normalization of the Haar measure μ. However, we plan to apply the corollary to $\Lambda = \mathcal{O}_K$ and want to replace $\operatorname{covol}(\mathcal{O}_K)$ with $\sqrt{|\operatorname{disc}(\mathcal{O}_K)|} = |D_K|^{1/2}$ via Proposition 14.15, which requires us to use the normalized Haar measure on $K_{\mathbb{R}}$ defined in §14.2.

19.1.1 Counting algebraic integers of bounded norm

Recall from §15.2 that the unit group $K_{\mathbb{R}}^\times$ of $K_{\mathbb{R}} \coloneqq K \otimes_{\mathbb{Q}} \mathbb{R}$ is the locally compact group

$$K_{\mathbb{R}}^\times \simeq \prod_{v|\infty} K_v^\times \simeq \prod_{\text{real } v|\infty} \mathbb{R}^\times \times \prod_{\text{complex } v|\infty} \mathbb{C}^\times.$$

We have a natural embedding

$$\begin{aligned} K^\times &\hookrightarrow K_{\mathbb{R}}^\times \\ x &\mapsto (x_v), \end{aligned}$$

where v ranges over the $r+s$ archimedean places of K; this allows us to view $K^\times$ as a subgroup of $K_{\mathbb{R}}^\times$ that contains the nonzero elements of $\mathcal{O}_K$. In Lecture 15 we defined the continuous homomorphism

$$\begin{aligned}\operatorname{Log} : K_{\mathbb{R}}^\times &\to \mathbb{R}^{r+s}\\ (x_v) &\mapsto (\log \|x_v\|_v),\end{aligned}$$

and proved that we have an exact sequence of abelian groups

$$1 \longrightarrow \mu_K \longrightarrow \mathcal{O}_K^\times \xrightarrow{\operatorname{Log}} \Lambda_K \to 0,$$

in which Λ_K is a lattice in the trace-zero hyperplane $\mathbb{R}_0^{r+s} := \{x \in \mathbb{R}^{r+s} : \mathrm{T}(x) = 0\}$ (where $\mathrm{T}(x)$ is the sum of the coordinates of x). The regulator R_K is the covolume of Λ_K in $\mathbb{R}_0^{r+s}$ (see Definition 15.16), where we endow $\mathbb{R}_0^{r+s}$ with the Euclidean measure induced by any coordinate projection $\mathbb{R}^{r+s} \to \mathbb{R}^{r+s-1}$. By Dirichlet's unit theorem (Theorem 15.12), we can write

$$\mathcal{O}_K^\times = U \times \mu_K,$$

where $U \subseteq \mathcal{O}_K^\times$ is free of rank $r+s-1$ (the subgroup U is not uniquely determined, but let us fix a choice).

We want to estimate the quantity

$$\#\{\mathfrak{a} : \mathrm{N}(\mathfrak{a}) \le t\},$$

where $\mathfrak{a}$ ranges over the nonzero ideals of $\mathcal{O}_K$, as $t \to \infty$. As a first step, let us restrict our attention to nonzero principal ideals $(\alpha) \subseteq \mathcal{O}_K$. We then want to estimate the cardinality of $\{(\alpha) : \mathrm{N}(\alpha) \le t\}$. We have $(\alpha) = (\alpha')$ if and only if $\alpha/\alpha' \in \mathcal{O}_K^\times$, so this is equivalent to

$$\{\alpha \in K^\times \cap \mathcal{O}_K : \mathrm{N}(\alpha) \le t\}/\mathcal{O}_K^\times,$$

where for any set $S \subseteq K_{\mathbb{R}}^\times$, the notation $S/\mathcal{O}_K^\times$ denotes the set of equivalence classes of S under the equivalence relation $\alpha \sim \alpha' \Leftrightarrow \alpha = u\alpha'$ for some $u \in \mathcal{O}_K^\times$. If we now define

$$K_{\mathbb{R},\le t}^\times := \{x \in K_{\mathbb{R}}^\times : \mathrm{N}(x) \le t\} \subseteq K_{\mathbb{R}}^\times \subseteq K_{\mathbb{R}},$$

then we want to estimate the cardinality of the finite set

$$\left(K_{\mathbb{R},\le t}^\times \cap \mathcal{O}_K\right)/\mathcal{O}_K^\times,$$

where the intersection takes place in $K_{\mathbb{R}}$ and produces a subset of $K_{\mathbb{R}}^\times$ that we partition into equivalence classes modulo $\mathcal{O}_K^\times$. To simplify matters, let us replace $\mathcal{O}_K^\times$ with the free group $U \subseteq \mathcal{O}_K^\times$; we then have a w_K–to–1 map

$$(K_{\mathbb{R},\le t}^\times \cap \mathcal{O}_K)/U \longrightarrow \left(K_{\mathbb{R},\le t}^\times \cap \mathcal{O}_K\right)/\mathcal{O}_K^\times.$$

It suffices to estimate the cardinality of $(K_{\mathbb{R},\le t}^\times \cap \mathcal{O}_K)/U$ and divide the result by w_K.

Recall that for $x = (x_v) \in K_{\mathbb{R}}^\times$, the norm map $\mathrm{N}\colon K_{\mathbb{R}}^\times \to \mathbb{R}_{>0}^\times$ is defined by

$$\mathrm{N}(x) := \prod_{v|\infty} \|x_v\|_v = \prod_{v \text{ real}} |x_v|_{\mathbb{R}} \prod_{v \text{ complex}} |x_v|_{\mathbb{C}}^2,$$

and satisfies $\mathrm{T}(\mathrm{Log}\, x) = \log \mathrm{N}(x)$ for all $x \in K_{\mathbb{R}}^{\times}$. We now define a surjective homomorphism

$$\begin{aligned} \nu\colon K_{\mathbb{R}}^{\times} &\twoheadrightarrow K_{\mathbb{R},1}^{\times} \\ x &\mapsto x\mathrm{N}(x)^{-1/n}. \end{aligned}$$

The image of $K_{\mathbb{R},1}^{\times}$ under the Log map is precisely the trace zero hyperplane $\mathbb{R}_0^{r+s}$ in $\mathbb{R}^{r+s}$ in which $\mathrm{Log}(U) = \mathrm{Log}(\mathcal{O}_K^{\times}) = \Lambda_K$ is a lattice. Let us fix a fundamental domain F for the lattice Λ_K in $\mathbb{R}_0^{r+s}$ so that

$$S := \nu^{-1}\left(\mathrm{Log}^{-1}(F)\right)$$

is a set of unique coset representatives for the quotient $K_{\mathbb{R}}^{\times}/U$. If we now define

$$S_{\le t} \coloneqq \{x \in S : \mathrm{N}(x) \le t\} \subseteq K_{\mathbb{R}},$$

we want to estimate the cardinality of the finite set

$$S_{\le t} \cap \mathcal{O}_K.$$

The set $\mathcal{O}_K$ is a lattice in the $\mathbb{R}$-vector space $K_{\mathbb{R}}$ of dimension n. We have $tS_{\le 1} = S_{\le t^n}$, so we can estimate the cardinality of $S_{\le t} = t^{1/n}S_{\le 1}$ via Corollary 19.6 with $S = S_{\le 1}$ and $\Lambda = \mathcal{O}_K$ by replacing t with $t^{1/n}$, provided that the boundary of $S_{\le 1}$ is $(n-1)$-Lipschitz parametrizable, which we now argue.

The kernel of the Log map is $\{\pm 1\}^r \times \mathrm{U}(1)^s$, where $\mathrm{U}(1) = \{z \in \mathbb{C} : z\bar{z} = 1\}$ is the unit circle in $\mathbb{C}$. We thus have a continuous isomorphism of locally compact groups

$$\begin{aligned} K_{\mathbb{R}}^{\times} = (\mathbb{R}^{\times})^r \times (\mathbb{C}^{\times})^s &\xrightarrow{\sim} \mathbb{R}^{r+s} \times \{\pm 1\}^r \times [0, 2\pi)^s \qquad (1) \\ x = (x_1, \dots, x_r, z_1, \dots, z_s) &\longmapsto (\mathrm{Log}\, x) \times (\operatorname{sgn} x_1, \dots, \operatorname{sgn} x_r) \times (\arg z_1, \dots, \arg z_s), \end{aligned}$$

where the map to $\mathbb{R}^{r+s}$ is the Log map, the map to $\{\pm 1\}^r$ is the vector of signs of the r real components, and the map to $[0, 2\pi)^s$ is the vector of angles $\arg z$ such that $z/|z| = e^{i \arg z}$ of the s complex components.

The set $S_{\le 1}$ consists of 2^r connected components, one for each element of $\{\pm 1\}^r$. We can parametrize each of these component using n real parameters as follows:

- $r + s - 1$ parameters in $[0, 1)$ that encode a point in F as an $\mathbb{R}$-linear combination of $\mathrm{Log}(\epsilon_1), \dots, \mathrm{Log}(\epsilon_{r+s-1})$, where $\epsilon_1, \dots, \epsilon_{r+s-1}$ are a basis for U;
- s parameters in $[0, 1)$ that encode an element of $\mathrm{U}(1)^s$;
- a parameter in $(0, 1]$ that encodes the nth-root of the norm.

These parameterizations define a continuously differentiable bijection from the set

$$C = [0, 1)^{n-1} \times (0, 1] \subseteq [0, 1]^n$$

to each of the 2^r disjoint components of $S_{\le 1}$; it can be written out explicitly in terms of exponentials and the identity function. The boundary ∂C is the boundary of the unit n-cube, which is clearly $(n-1)$-Lipschitz parametrizable; thus each component of $S_{\le 1}$, and therefore $S_{\le 1}$ itself, is $(n-1)$-Lipschitz parametrizable.

We now apply Corollary 19.6 to the lattice $\mathcal{O}_K$ and the set $S_{\le 1}$ in the n-dimensional $\mathbb{R}$-vector space $K_{\mathbb{R}}$ with t replaced by $t^{1/n}$, since $S_{\le t} = t^{1/n}S_{\le 1}$. This yields

$$\#(S_{\le t} \cap \mathcal{O}_K) = \frac{\mu(S_{\le 1})}{\mathrm{covol}(\mathcal{O}_K)}(t^{1/n})^n + O\big((t^{1/n})^{n-1}\big) = \left(\frac{\mu(S_{\le 1})}{|D_K|^{1/2}}\right) t + O\big(t^{1-1/n}\big). \qquad (2)$$

Our next task is compute $\mu(S_{\le 1})$; as noted in Remark 19.7, we must use the normalized Haar measure μ on $K_{\mathbb{R}}$ defined in §14.2 when doing so. We will use the isomorphism in (1) to make a change of coordinates, we just need to understand how this affects the Haar measure μ on $K_{\mathbb{R}} = \prod_{v|\infty} K_v \simeq \mathbb{R}^r \times \mathbb{C}^s$. In terms of the standard Lebesgue measures dx and dA on $\mathbb{R}$ and $\mathbb{C}$, we have $\mu = (dx)^r(2dA)^s$, where the $2dA$ reflects the fact that the normalized absolute value $\| \ \|_v$ for each complex place v is the square of the Euclidean absolute value on $\mathbb{C}$. For each factor of $K_{\mathbb{R}}^\times = \prod_{v|\infty} K_v \simeq (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s \subseteq \mathbb{R}^r \times \mathbb{C}^s$ we define the maps

$$\begin{aligned} \mathbb{R}^\times &\to \mathbb{R} \times \{\pm 1\} & \mathbb{C}^\times &\to \mathbb{C} \times [0, 2\pi) \\ x &\mapsto (\log|x|, \operatorname{sgn} x) & z &\mapsto (2\log|z|, \arg z) \\ \pm e^\ell &\leftarrow\!\shortmid (\ell, \pm 1) & e^{\ell/2+i\theta} &\leftarrow\!\shortmid (\ell, \theta) \\ dx &\mapsto e^\ell d\ell \mu_{\{\pm 1\}} & 2dA &\mapsto 2e^{\ell/2} d(e^{\ell/2}) d\theta = e^\ell d\ell d\theta, \end{aligned}$$

where $d\ell$ is the Lebesgue measure on $\mathbb{R}$, $\mu_{\{\pm 1\}}$ is the counting measure on $\{\pm 1\}$, and $d\theta$ is the Lebesgue measure on $[0, 2\pi)$. We thus have

$$\begin{aligned} K_{\mathbb{R}}^\times &\xrightarrow{\sim} \mathbb{R}^{r+s} \times \{\pm 1\}^r \times [0, 2\pi)^s \\ \mu &\mapsto e^{\mathrm{T}(\cdot)} \mu_{\mathbb{R}^{r+s}} \mu_{\{\pm 1\}}^r \mu_{[0,2\pi)}^s, \end{aligned}$$

where the trace function $\mathrm{T}(\cdot)$ sums the coordinates of a vector in $\mathbb{R}^{r+s}$.

We now make one further change of coordinates:

$$\begin{aligned} \mathbb{R}^{r+s} &\to \mathbb{R}^{r+s-1} \times \mathbb{R} \\ x = (x_1, \dots, x_{r+s}) &\mapsto (x_1, \dots, x_{r+s-1}, y := \mathrm{T}(x)) \\ e^{\mathrm{T}(x)} \mu_{\mathbb{R}^{r+s}} &\mapsto e^y \mu_{\mathbb{R}^{r+s-1}} dy. \end{aligned}$$

If we let $\pi\colon \mathbb{R}^{r+s} \to \mathbb{R}^{r+s-1}$ denote the coordinate projection, then the measure of $\pi(F)$ in $\mathbb{R}^{r+s-1}$ is, by definition, the regulator R_K (see Definition 15.16).

The Log map gives us a bijection

$$\begin{aligned} S_{\le 1} &\xrightarrow{\sim} F + (-\infty, 0] \left(\frac{1}{n}, \dots, \frac{1}{n}, \frac{2}{n}, \dots, \frac{2}{n}\right), \\ x = \mathrm{N}(x)^{1/n} \nu(x) &\mapsto \mathrm{Log}\, \nu(x) + \log \mathrm{N}(x) \left(\frac{1}{n}, \dots, \frac{1}{n}, \frac{2}{n}, \dots, \frac{2}{n}\right). \end{aligned}$$

The coordinate $y \in (-\infty, 0]$ is given by $y = \mathrm{T}(\mathrm{Log}\, x) = \log \mathrm{N}(x)$, so we can view $S_{\le 1}$ as an infinite union of cosets of $\mathrm{Log}^{-1}(F)$ parameterized by $e^y = \mathrm{N}(x) \in (0, 1]$.

Under our change of coordinates we thus have

$$\begin{aligned} K_{\mathbb{R}}^\times &\xrightarrow{\sim} \mathbb{R}^{r+s-1} \times \mathbb{R} \times \{\pm 1\}^r \times [0, 2\pi)^s \\ S_{\le 1} &\to \pi(F) \times (-\infty, 0] \times \{\pm 1\}^r \times [0, 2\pi)^s. \end{aligned}$$

Since $R_K = \mu_{\mathbb{R}^{r+s-1}}(\pi(F))$, we have

$$\begin{aligned} \mu(S_{\le 1}) &= \int_{-\infty}^0 e^y R_K 2^r (2\pi)^s dy \\ &= 2^r (2\pi)^s R_K. \end{aligned}$$

Plugging this into (2) yields

$$\#(S_{\le t} \cap \mathcal{O}_K) = \left(\frac{2^r (2\pi)^s R_K}{|D_K|^{1/2}}\right) t + O\left(t^{1-1/n}\right). \tag{3}$$

19.2 Proof of the analytic class number formula

We are now ready to prove the analytic class number formula. Our main tool is the following theorem, which uses our analysis in the previous section to give a precise asymptotic estimate on the number of ideals of bounded norm.

Theorem 19.8. *Let K be a number field of degree n As $t \to \infty$, the number of nonzero $\mathcal{O}_K$-ideals $\mathfrak{a}$ of absolute norm $\mathrm{N}(\mathfrak{a}) \le t$ is*

$$\left(\frac{2^r(2\pi)^s h_K R_K}{w_k |D_K|^{1/2}}\right) t + O\left(t^{1-1/n}\right),$$

where r and s are the number of real and complex places of K, respectively, $h_K = \#\operatorname{cl}\mathcal{O}_K$ is the class number, R_K is the regulator, $w_K := \#\mu_K$ is the number of roots of unity, and $D_K := \operatorname{disc}\mathcal{O}_K$ is the absolute discriminant.

Proof. In order to count the nonzero $\mathcal{O}_K$-ideals $\mathfrak{a}$ of absolute norm $\mathrm{N}(\mathfrak{a}) \le t$ we group them by ideal class. For the trivial class, we just need to count nonzero principal ideals (α), equivalently, the number of nonzero $\alpha \in \mathcal{O}_K$ with $\mathrm{N}(\alpha) \le t$, modulo the unit group $\mathcal{O}_K^\times$. Dividing (3) by w_K to account for the w_K-to-1 map

$$S_{\le t} \cap \mathcal{O}_K \longrightarrow (K^\times_{\mathbb{R},\le t} \cap \mathcal{O}_K)/\mathcal{O}_K^\times,$$

we obtain

$$\#\{(\alpha) \subseteq \mathcal{O}_K : \mathrm{N}(\alpha) \le t\} = \left(\frac{2^r(2\pi)^s R_K}{w_K |D_K|^{1/2}}\right) t + O\left(t^{1-1/n}\right). \tag{4}$$

To complete the proof we now show that we get the same answer for every ideal class; the nonzero ideals $\mathfrak{a}$ of norm $\mathrm{N}(\mathfrak{a}) \le t$ are asymptotically equidistributed among ideal classes.

Fix an ideal class $[\mathfrak{a}]$, with $\mathfrak{a} \subseteq \mathcal{O}_K$ nonzero (every ideal class contains an integral ideal, by Theorem 14.19). Multiplication by $\mathfrak{a}$ gives a bijection

$$\begin{aligned}\{\text{ideals } \mathfrak{b} \in [\mathfrak{a}^{-1}] : \mathrm{N}(\mathfrak{b}) \le t\} &\xrightarrow{\times\mathfrak{a}} \{\text{nonzero principal ideals } (\alpha) \subseteq \mathfrak{a} : \mathrm{N}(\alpha) \le t\mathrm{N}(\mathfrak{a})\} \\ &\longrightarrow \{\text{nonzero } \alpha \in \mathfrak{a} : \mathrm{N}(\alpha) \le t\mathrm{N}(\mathfrak{a})\}/\mathcal{O}_K^\times.\end{aligned}$$

Let $S_{[\mathfrak{a}],\le t}$ denote the set on the RHS. The estimate in (4) derived from Corollary 19.6 applies to any lattice in $K_\mathbb{R}$, not just $\mathcal{O}_K$. Replacing $\mathcal{O}_K$ with $\mathfrak{a}$ in (4) we obtain

$$\begin{aligned}\#S_{[\mathfrak{a}],\le t} &= \left(\frac{2^r(2\pi)^s R_K}{w_k \operatorname{covol}(\mathfrak{a})}\right) t\,\mathrm{N}(\mathfrak{a}) + O\big(t^{1-1/n}\big) \\ &= \left(\frac{2^r(2\pi)^s R_K}{w_k \operatorname{covol}(\mathcal{O}_K)\mathrm{N}(\mathfrak{a})}\right) t\,\mathrm{N}(\mathfrak{a}) + O\big(t^{1-1/n}\big) \\ &= \left(\frac{2^r(2\pi)^s R_K}{w_k |D_K|^{1/2}}\right) t + O\big(t^{1-1/n}\big),\end{aligned}$$

since $\operatorname{covol}(\mathfrak{a}) = N(\mathfrak{a})\operatorname{covol}(\mathcal{O}_K)$, by Corollary 14.16. Note that the RHS does not depend on the ideal class $[\mathfrak{a}]$. Summing over ideal classes yields

$$\#\{\text{nonzero ideals } \mathfrak{b} \subseteq \mathcal{O}_K : \mathrm{N}(\mathfrak{b}) \le t\} = \sum_{[\mathfrak{a}] \in \mathrm{cl}(\mathcal{O}_K)} \#S_{[\mathfrak{a}],\le t} = \left(\frac{2^r(2\pi)^s h_K R_K}{w_K |D_K|^{1/2}}\right) t + O\left(t^{1-1/n}\right),$$

as claimed. □

Lemma 19.9. *Let $a_1, a_2, \dots$ be a sequence of complex numbers and let σ be a real number. Suppose that*

$$a_1 + \cdots + a_t = O(t^\sigma) \qquad (\text{as } t \to \infty).$$

Then the Dirichlet series $\sum a_n n^{-s}$ defines a holomorphic function on $\operatorname{Re} s > \sigma$.

Proof. Let $A(x) := \sum_{0<n\le x} a_n$. Writing the Dirichlet sum as a Stieltjes integral (apply Corollary 18.27 with $f(n) = n^{-s}$ and $g(n) = a_n$), for $\operatorname{Re}(s) > \sigma$ we have

$$\begin{aligned}\sum_{n=1}^{\infty} a_n n^{-s} &= \int_{1^-}^{\infty} x^{-s}\, dA(x)\\ &= \frac{A(x)}{x^s}\Big|_{1^-}^{\infty} - \int_{1^-}^{\infty} A(x)\, dx^{-s}\\ &= (0-0) - \int_{1^-}^{\infty} A(x)(-sx^{-s-1})\, dx\\ &= s\int_{1^-}^{\infty} \frac{A(x)}{x^{s+1}}\, dx.\end{aligned}$$

Note that we used $|A(x)| = O(x^\sigma)$ and $\operatorname{Re}(s) > \sigma$ to conclude $\lim_{x\to\infty} A(x)/x^s = 0$. The integral on the RHS converges locally uniformly on $\operatorname{Re}(s) > \sigma$ and the lemma follows. □

Remark 19.10. Lemma 19.9 gives us an *abscissa of convergence* σ for the Dirichlet series $\sum a_n n^{-s}$; this is analogous to the radius of convergence of a power series.

Lemma 19.11. *Let $a_1, a_2, \dots$ be a sequence of complex numbers that satisfies*

$$a_1 + \cdots + a_t = \rho t + O(t^\sigma) \qquad (\text{as } t \to \infty)$$

for some $\sigma \in [0,1)$ and $\rho \in \mathbb{C}^\times$. The Dirichlet series $\sum a_n n^{-s}$ converges on $\operatorname{Re}(s) > 1$ and has a meromorphic continuation to $\operatorname{Re}(s) > \sigma$ that is holomorphic except for a simple pole at $s = 1$ with residue ρ.

Proof. Define $b_n := a_n - \rho$. Then $b_1 + \cdots + b_t = O(t^\sigma)$ and

$$\sum a_n n^{-s} = \rho \sum n^{-s} + \sum b_n n^{-s} = \rho\,\zeta(s) + \sum b_n n^{-s}.$$

We have already proved that the Riemann zeta function $\zeta(s)$ is holomorphic on $\operatorname{Re}(s) > 1$ and has a meromorphic continuation to $\operatorname{Re}(s) > 0$ that is holomorphic except for a simple pole at 1 with residue 1. By the previous lemma, $\sum b_n n^{-s}$ is holomorphic on $\operatorname{Re}(s) > \sigma$, and since $\sigma < 1$, it is holomorphic at $s = 1$. So the entire RHS has a meromorphic continuation to $\operatorname{Re}(s) > \sigma$ that is holomorphic except for the simple pole at 1 coming from $\zeta(s)$, and the residue at $s = 1$ is $\rho \cdot 1 + 0 = \rho$. □

We are now ready to prove the analytic class number formula.

Theorem 19.12 (Analytic Class Number Formula)**.** *Let K be a number field of degree n. The Dedekind zeta function $\zeta_K(z)$ extends to a meromorphic function on $\operatorname{Re}(z) > 1 - \frac{1}{n}$ that is holomorphic except for a simple pole at $z = 1$ with residue*

$$\lim_{z\to 1^+} (z-1)\zeta_K(z) = \rho_K := \frac{2^r (2\pi)^s h_K R_K}{w_K |D_K|^{1/2}},$$

where r and s are the number of real and complex places of K, respectively, $h_K := \#\operatorname{cl}\mathcal{O}_K$ is the class number, R_K is the regulator, $w_K := \mu_K$ is the number of roots of unity, and $D_K := \operatorname{disc}\mathcal{O}_K$ is the absolute discriminant.

Proof. We have

$$\zeta_K(z) = \sum_{\mathfrak{a}} \mathrm{N}(\mathfrak{a})^{-z} = \sum_{t \geq 1} a_t t^{-z},$$

where $\mathfrak{a}$ ranges over nonzero ideals of $\mathcal{O}_K$, and $a_t := \#\{\mathfrak{a} : \mathrm{N}(\mathfrak{a}) = t\}$ with $t \in \mathbb{Z}_{\geq 1}$. If we now define

$$\rho_K := \frac{2^r (2\pi)^s h_K R_K}{w_K |D_K|^{1/2}},$$

then by Theorem 19.8 we have

$$a_1 + \cdots + a_t = \#\{\mathfrak{a} : \mathrm{N}(\mathfrak{a}) \leq t\} = \rho_K t + O(t^{1-1/n}) \qquad (\text{as } t \to \infty).$$

Applying Lemma 19.11 with $\sigma = 1 - 1/n$, we see that $\zeta_K(z) = \sum a_t t^{-z}$ extends to a meromorphic function on $\mathrm{Re}(z) > 1 - 1/n$ that is holomorphic except for a simple pole at $z = 1$ with residue ρ_K. □

Remark 19.13. As previously noted, Hecke proved that $\zeta_K(z)$ extends to a meromorphic function on $\mathbb{C}$ with no poles other than the simple pole at $z = 1$, and it satisfies a functional equation. If we define the *gamma factors*[1]

$$\Gamma_{\mathbb{R}}(z) := \pi^{-z/2}\Gamma\left(\tfrac{z}{2}\right), \qquad \text{and} \qquad \Gamma_{\mathbb{C}}(z) := \Gamma_{\mathbb{R}}(z)\Gamma_{\mathbb{R}}(z+1) = 2(2\pi)^{-z}\Gamma(z),$$

and the *completed zeta function*

$$\xi_K(z) := |D_K|^{z/2}\Gamma_{\mathbb{R}}(z)^r \Gamma_{\mathbb{C}}(z)^s \zeta_K(z),$$

where r and s are the number of real and complex places of K, respectively, then $\xi_K(z)$ is holomorphic except for simple poles at $z = 0, 1$ and satisfies the *functional equation*

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

In the case $K = \mathbb{Q}$, we have $r = 1$ and $s = 0$, so

$$\xi_{\mathbb{Q}}(z) = \Gamma_{\mathbb{R}}(z)\zeta(z) = \pi^{-z/2}\Gamma(\tfrac{z}{2})\zeta_{\mathbb{Q}}(z),$$

which is precisely the completed zeta function $Z(z)$ we defined for the Riemann zeta function $\zeta(z) = \zeta_{\mathbb{Q}}(z)$ in Lecture 17 (without any extra factors to remove the zeros at $z = 0, 1$).

19.3 Cyclotomic zeta functions and Dirichlet L-functions

Having proved the analytic class number formula, we now want to complete the proof of Dirichlet's theorem on primes in arithmetic progressions that we began in the previous lecture. To do this we need to establish a connection between Dirichlet L-functions and Dedekind zeta functions of cyclotomic fields.

Recall from Problem Set 4 that we have an isomorphism $\varphi\colon \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^\times$ canonically defined by $\sigma(\zeta_m) = \zeta_m^{\varphi(\sigma)}$ (independent of the choice of ζ_m). The canonical bijection given by Corollary 18.16 allows us to identify the set $X(m)$ of primitive Dirichlet characters of conductor dividing m with the character group of $(\mathbb{Z}/m\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$.[2]

[1] The rightmost equality follows from the duplication formula for $\Gamma(s)$. In older texts one may find $\Gamma_{\mathbb{C}}(s)$ defined as $(2\pi)^{-z}\Gamma(z)$, which yields the same functional equation.

[2] As noted in Remark 18.17, the group operation on $X(m)$ is not pointwise multiplication, one multiplies elements of $X(m)$ by taking the unique primitive character that induces the pointwise product.

More generally, given any finite set of primitive Dirichlet characters, if we let m be the LCM of their conductors and consider the subgroup H of $X(m)$ they generate, we may associate to H the subfield $K := \mathbb{Q}(\zeta_m)^{\phi(H)}$, where

$$\phi(H) := \{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) : \chi(\sigma) = 1 \text{ for all } \chi \in H\};$$

we may then regard H as the character group of $\mathrm{Gal}(K/\mathbb{Q})$ via Proposition 18.39. The same applies if we replace m with any multiple m', since $H \subseteq X(m) \subseteq X(m')$ for all $m|m'$ and we will get the same field $K \subseteq \mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_{m'})$.

Conversely, for each subfield K of a cyclotomic field $\mathbb{Q}(\zeta_m)$ there is a corresponding subgroup

$$H := \{\chi \in X(m) : \chi(\sigma) = 1 \text{ for all } \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/K)\},$$

for which $K = \mathbb{Q}(\zeta_m)^{\phi(H)}$. Note that $K/\mathbb{Q}$ is Galois, since $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is abelian (every subgroup is normal), and we may view H as the character group of $\mathrm{Gal}(K/\mathbb{Q})$. We thus have a one-to-one correspondence between subgroups $H \subseteq X(m)$ and subfields of $K \subseteq \mathbb{Q}(\zeta_m)$ in which H corresponds to the character group of $\mathrm{Gal}(K/\mathbb{Q})$ and $K = \mathbb{Q}(\zeta_m)^{\phi(H)}$.

We will prove that under this correspondence, the Dedekind zeta function of $\zeta_K(s)$ is the product of the Dirichlet L-functions $L(s,\chi)$ for $\chi \in H$. We first note the following.

Proposition 19.14. *Let p be a prime, let m be a positive integer, and let $m' = m/p^{v_p(m)}$. Then $\mathbb{Q}(\zeta_{m'})$ is the maximal extension of $\mathbb{Q}$ in $\mathbb{Q}(\zeta_m)$ unramified at p. In particular, if p does not divide m then $\mathbb{Q}(\zeta_m)$ is unramified at p.*

Proof. By Corollary 10.20, the extension $\mathbb{Q}_p(\zeta_{m'})/\mathbb{Q}_p$ is unramified. It follows from Proposition 12.4 that $\mathbb{Q}(\zeta_{m'})/\mathbb{Q}$ is unramified at p. Applying the same argument to all primes $q \neq p$ dividing m shows that the extension $\mathbb{Q}(\zeta_{p^{v_p(m)}})$ is ramified only at p. By Corollary 14.25, there are no nontrivial unramified extensions of $\mathbb{Q}$, so every subfield of $\mathbb{Q}(\zeta_{p^{v_p(m)}})$ that properly contains $\mathbb{Q}$ is ramified at p. Now $\mathbb{Q}(\zeta_m)$ is the compositum of $\mathbb{Q}(\zeta_{p^{v_p(m)}})$ and $\mathbb{Q}(\zeta_{m'})$, which intersect in $\mathbb{Q}$, so any nontrivial extension of $\mathbb{Q}(\zeta'_m)$ in $\mathbb{Q}(\zeta_m)$ contains a subfield of $\mathbb{Q}(\zeta_{p^{v_p(m)}})$ properly containing $\mathbb{Q}$ which must be ramified at p; the proposition follows. □

Theorem 19.15. *Let $H \subseteq X(m)$ be a group of primitive Dirichlet characters and let $K = \mathbb{Q}(\zeta_m)^{\phi(H)}$ be the corresponding subfield of $\mathbb{Q}(\zeta_m)$, with $\phi(H)$ defined as above. Then*

$$\zeta_K(s) = \prod_{\chi \in H} L(s,\chi).$$

Proof. On the LHS we have

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \mathrm{N}(\mathfrak{p})^{-s}\right)^{-1} = \prod_{p} \prod_{\mathfrak{p}|p} \left(1 - \mathrm{N}(\mathfrak{p})^{-s}\right)^{-1},$$

and on the RHS we have

$$\prod_{\chi \in H} L(s,\chi) = \prod_{\chi \in H} \prod_{p} \left(1 - \chi(p)p^{-s}\right)^{-1} = \prod_{p} \prod_{\chi \in H} \left(1 - \chi(p)p^{-s}\right)^{-1}.$$

It thus suffices to prove

$$\prod_{\mathfrak{p}|p} \left(1 - \mathrm{N}(\mathfrak{p})^{-s}\right) \stackrel{?}{=} \prod_{\chi \in H} \left(1 - \chi(p)p^{-s}\right) \tag{5}$$

for each prime p.

Since $K/\mathbb{Q}$ is Galois, we have $[K:\mathbb{Q}] = e_p f_p g_p$, where e_p is the ramification index, f_p is the residue field degree, and $g_p = \#\{\mathfrak{p}|p\}$. On the LHS of (5) we have

$$\prod_{\mathfrak{p}|p} \left(1 - \mathrm{N}(\mathfrak{p})^{-s}\right) = \left(1 - (p^{f_p})^{-s}\right)^{g_p} = \left(1 - (p^{-s})^{f_p}\right)^{g_p},$$

which we note does not change if we replace K with the maximal subfield K' of K in which p is unramified (since K/K' is totally ramified at every prime of K' above p, only e_p changes, not f_p or g_p). On the RHS of (5), we have $\chi(p) = 0$ for all $\chi \in H$ with conductor divisible by p, so we can replace H with the subgroup H' of Dirichlet characters with conductors prime to p. It follows from Proposition 19.14 that $K' = \mathbb{Q}(\zeta_m)^{\phi(H')}$ (to see this, note that if we put $m' = m/p^{v_p(m)}$ then $K' = K \cap \mathbb{Q}(\zeta_{m'})$ and $H' = H \cap X(m')$). Thus without loss of generality we assume $p \nmid m$, so K is unramified at p and we have $\#H = [K:\mathbb{Q}] = f_p g_p$.

Since $K/\mathbb{Q}$ is abelian and unramified at p, the Artin map gives us a Frobenius element σ_p corresponding to the Frobenius automorphism $x \mapsto x^p$ of the residue field, which by definition has order f_p, so σ_p has order f_p in $\mathrm{Gal}(K/\mathbb{Q})$. Viewing H as the character group of $\mathrm{Gal}(K/\mathbb{Q})$, the map $\chi \mapsto \chi(\sigma_p)$ defines a surjective homomorphism from H to the group of f_p-th roots of unity $\alpha \in \mathrm{U}(1)$, and the kernel of this map has cardinality $\#H/f_p = g_p$. Therefore

$$\prod_{\chi \in H} \left(1 - \chi(p)p^{-s}\right) = \prod_{\alpha^{f_p}=1} \left(1 - \alpha p^{-s}\right)^{g_p} = \left(1 - (p^{-s})^{f_p}\right)^{g_p},$$

where the second equality follows from the identity $\prod_{\alpha^{f_p}=1}(1 - \alpha T) = 1 - T^{f_p} \in \mathbb{C}[T]$. □

19.4 Non-vanishing of Dirichlet L-functions with non-principal character

We are now ready to prove the key claim needed to complete our proof of Dirichlet's theorem on primes in arithmetic progressions.

Theorem 19.16. *Let ψ be any non-principal Dirichlet character. Then $L(1,\psi) \neq 0$.*

Proof. Let ψ be a non-principal Dirichlet character, say of modulus m. Then ψ is induced by a non-trivial primitive Dirichlet character $\widetilde{\psi}$ of conductor $\widetilde{m}$ dividing m. The L-functions of ψ and $\widetilde{\psi}$ differ at only finitely many Euler factors $(1 - \psi(p)p^{-s})^{-1}$ (corresponding to primes p dividing $m/\widetilde{m}$), and these factors are clearly nonzero at $s = 1$, since $p > 1$. We thus assume without loss of generality that $\psi = \widetilde{\psi}$ is primitive.

Let K be the mth cyclotomic field $\mathbb{Q}(\zeta_m)$. By Theorem 19.15 we have

$$\zeta_K(s) = \prod_{\chi} L(s,\chi),$$

where χ ranges over the primitive Dirichlet characters of conductor dividing m, including ψ. By the analytic class number formula (Theorem 19.12), the LHS has a simple pole at $s = 1$,

and the same must be true of the RHS. Thus

$$\begin{aligned}\operatorname{ord}_{s=1}\zeta_K(s) &= \operatorname{ord}_{s=1}\prod_{\chi} L(s,\chi)\\ -1 &= \operatorname{ord}_{s=1}L(s,\mathbb{1})\prod_{\chi\neq\mathbb{1}} L(s,\chi)\\ -1 &= \operatorname{ord}_{s=1}\zeta(s)\prod_{\chi\neq\mathbb{1}} L(s,\chi)\\ -1 &= -1+\sum_{\chi\neq\mathbb{1}}\operatorname{ord}_{s=1}L(s,\chi).\end{aligned}$$

Each $\chi \neq \mathbb{1}$ in the sum is necessarily non-principal (since it is primitive). We proved in Proposition 18.20 that for non-principal χ the Dirichlet L-series $L(s,\chi)$ is holomorphic on $\operatorname{Re}(s) > 0$, thus $\operatorname{ord}_{s=1}L(s,\chi) \geq 0$ for all χ appearing in the sum, which can therefore be zero if and only if every term $\operatorname{ord}_{s=1}L(s,\chi)$ is zero. So $L(1,\chi) \neq 0$ for every non-trivial primitive Dirichlet character χ of conductor dividing m, including ψ. □

References

[1] Erich Hecke, *Über die Zetafunktion beliebiger algebraischer Zahlkörper*, Nachr. Ges. Wiss. Göttingen (1917), 77–89.

[2] P.G. Lejeune Dirichlet and Richard Dedekind, *Vorlesungun über Zahlentheorie*, Braunschweig F. Veiweg, 1894.

[3] Edmund Landau, *Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes*, Math. Ann. **56**, 645–670.

18.785 Number Theory I
Fall 2019