MAT417 Lecture Notes

Isaac Clark

September 5, 2025

1 Day 1 - Motivating results

1.1 Introduction

The guiding questions that we will seek to answer in this course concern the structure of the prime numbers. More specifically, (1) how many prime numbers are there? and (2) what can we say about the distribution of primes? More carefully, putting $\pi(x) = |\{p \leq x \mid p \text{ prime}\}|$, can we estimate $\pi(x)$?

1.2 The Prime Number theorem

One simple answer is that $\pi(x) \to \infty$ as $x \to \infty$ due to the infinitude of primes. Doing better, the Prime Number theorem asserts $\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1$ (*Exercise.* Use the Prime Number theorem to show that the "size" of the n-th prime is $n \log n$).

Again by the Prime Number theorem, $\pi(x)/x \to 0$, so the primes have zero asymptoic density, but the density tends to 0 very slowly.

1.3 Dirichlet's theorem

Another important theorem about the density of primes is due to Dirichlet. Fix $a, d \in \mathbb{N}$ coprime. Then there are infinitely many primes of the form $a + kd$ for $k \in \mathbb{N}$. (*Note.* This is, in a sense, a negative result to the question of an underlying structure of primes "favouring" certain congruences).

1.4 A (Bad) Lower Bound for $\pi(x)$

Using Euclid's argument for the infinitude of primes, if p_n is the n-th prime then $p_{n+1} \leq 1 + \prod_{i=1}^{n} p_i \leq 2 \prod_{i=1}^{n} p_i$. An inductive argument yields $p_n < 2^{2^{n-1}}$ taking

logarithms then yields $\pi(x) > \log_2 \log_2 x$.

1.5 The Riemann ζ-Function

Put $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$. Restricting to $s \in \mathbb{R}$ for now, by the integral test, $\zeta(s)$ is absolutely convergent if and only if $s > 1$.

Observe. By using the Taylor series of $(1-x)^{-1}$, expanding, and an argument by prime factorizations, we have

$$\prod_{p \text{ prime}} (1 - p^{-s})^{-1} = \prod_{p \text{ prime}} \sum_{k=0}^{\infty} p^{-ks} = \sum_{\substack{p_1 < \cdots < p_n \text{ prime} \\ a_1, \ldots, a_n \geq 0}} (p_1^{a_1} \cdots p_n^{a_n})^{-s} = \sum_{n=1}^{\infty} n^{-s}$$

Remark. Since the harmonic series diverges, the above yields another proof that there are infinitely many primes.

Next time. We'll upgrade this argument to show that $\sum_{p \text{ prime}} 1/p$ diverges, concluding that we cannot bound $\pi(x)$ by any Cx^{θ} with $\theta < 1$.

2 Day 2 - $\sum_p 1/p$, Dirichlet series, and L-functions

2.1 $\sum_p 1/p$ diverges

From here on out a p in the subscript of a sum or product will mean p prime. Recall $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$. By running through the integral test, i.e. comparing $\zeta(s)$ to suitable upper and lower sums of $\int_1^{\infty} x^{-s}\, dx$, we get the bound:

$$(s-1)^{-1} < \zeta(s) < 1 + (s-1)^{-1} \tag{2.1}$$

Recall also that $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$. Then $\log(\zeta(s)) = -\sum_p \log(1 - p^{-s})^{-1}$.

Lemma 2.1. *$\forall s_0 > 1\ \exists M > 0$ such that $\forall 1 < s \leq s_0$, $\left|\sum_p p^{-s} - \log((s-1)^{-1})\right| < M$.*

Proof. Since log is order preserving, by (2.1):

$$-\log(s-1) < -\sum_p \log(1 - p^{-s}) < \log(s) - \log(s-1) \tag{2.2}$$

$$0 < \log(s-1) - \sum_p \log(1 - p^{-s}) < \log(s) \tag{2.3}$$

By Taylor expanding $\log(1+y)$ about $y=0$ and plugging in $y=p^{-s}$ yields

$$\left|p^{-s}+\log(1-p^{-s})\right| < p^{-2s} \tag{2.4}$$

Applying the triangle inequality to the partial sums and passing to limits,

$$\left|\sum_p p^{-s}+\sum_p \log(1-p^{-s})\right| \leq \sum_p |p^{-s}+\log(1-p^{-s})| < \sum_p p^{-2s} < \zeta(2) \tag{2.5}$$

Since $s>1$. Finally,

$$\begin{aligned}\left|\sum_p p^{-s}+\log(s-1)\right| &\leq \left|\sum_p p^{-s}+\sum_p \log(1-p^{-s})\right| + \left|\log(s-1)-\sum_p \log(1-p^{-s})\right| \\ &< \zeta(2)+\log(s) \text{ , by (2.3) and (2.5)} \\ &\leq \zeta(2)+s_0-1 \text{ , for } 1<s\leq s_0\end{aligned}$$

Thus, $M=\zeta(2)+s_0-1$ is as desired. □

Theorem 2.1. *$\sum_p 1/p$ diverges.*

Proof. An equivalent formulation of **Lemma 2.1** is $\sum_p p^{-s} = \log(s-1)+O(1)$. Roughly speaking (the precise formulation is an exercise) as $s\to 1^+$, $\log(s-1)\to\infty$ and, since $O(1)$ is bounded, so does the right hand side. Thus, the left hand side diverges as $s\to 1^+$ and so we have the claim. □

2.2 Dirichlet series and L-functions

For $m\in\mathbb{N}$, let $(\mathbb{Z}/m\mathbb{Z})^*$ be the invertible elements in the ring $\mathbb{Z}/m\mathbb{Z}$ regarded as a group under multiplication. A character on $\mathbb{Z}/m\mathbb{Z}$, or indeed, any finite abelian group, is a group homomorphism from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{C}^*$, the multiplicative group of complex numbers. Fix a character $\overline{\chi}$ on $\mathbb{Z}/m\mathbb{Z}$. We can extend $\overline{\chi}$ to a map $\mathbb{Z}\to\mathbb{C}$ by

$$\chi(n) = \begin{cases} 0 \text{ , if } (n,m)\neq 1 \\ \overline{\chi}(n \bmod m) \text{ , if } (n,m)=1 \end{cases}$$

Note. For all $m\in\mathbb{N}$ there is the trivial homomorphism $(\mathbb{Z}/m\mathbb{Z})^*\to\mathbb{C}^*$. The corresponding χ is the indicator on the integers coprime to m. I have heard this referred to as the principal Dirichlet character of modulus m, though it was not given a name in lecture. Going forward, for the forseeable future at least, I will use character to refer

to both group characters and Dirichlet characters despite the latter technically being an arithmetic function, as well as using χ to denote both, and trust the reader to infer which is correct.

Definition. For a fixed Dirichlet character χ, put $L(\chi, s) = \sum_{n=1}^{\infty} \chi(s) n^{-s}$. $L(\chi, s)$ is called a Dirichlet L-function.

Theorem 2.2. *$L(\chi, s)$ is absolutely convergent for $\mathfrak{Re}(s) > 1$*

Proof. Let $\overline{\chi}$ be the character on $(\mathbb{Z}/m\mathbb{Z})^*$ such that χ is the corresponding Dirichlet character. For each n coprime to m,

$$1 = |1| = |\overline{\chi}(1)| = |\overline{\chi}(n^m)| = |\overline{\chi}(n)|^m$$

So $|\overline{\chi}(n)| = 1$. Then, for any $n \in \mathbb{Z}$, $|\chi(n)| \leq |\overline{\chi}(n)| = 1$, so $|L(\chi, s)| \leq \zeta(s) < \infty$. $\square$

Over the next few lectures, we will be building up to the following theorem.

Theorem 2.3. *Let χ be a character.*

1. *$L(\chi, s)$ is holomorphic for $\mathfrak{Re}(s) > 1$.*
2. *For χ non-principal, $L(\chi, s)$ coverges and is holomorphic for $\mathfrak{Re}(s) > 0$.*
3. *For χ non-principal, $L(\chi, 1) \neq 0$.*

In preparation, we will prove a few useful lemmas.

Lemma 2.2. *For G a finite abelian group, all characters $\chi : G \to \mathbb{C}^*$, denoted by $G^\vee$, form a group under pointwise multiplication. Then,*

1. *$G^\vee \simeq G$.*
2. *$(G^\vee)^\vee \cong G$.*
3. *$(G \times H)^\vee \simeq G^\vee \times H^\vee$, for H another finite abelian group.*

Note. Here, $\simeq$ denotes non-canonically isomorphic, i.e. every isomorphism requires a "choice" and there is no "preferred choice". For example, a finite-dimensional vector space is non-canonically isomorphic to its dual space, since there is no basis-independent isomorphism. We denote canonically isomorphic by $\cong$. Returning to the example of vector spaces, every vector space is canonically isomorphic to its double dual via the association of $v \in V$ to its evaluation map $\widehat{v} : \varphi \mapsto \varphi(v)$.

Proof. Let $\iota_G : G \to G \times H$ be given by $\iota_G(g) = (g, 1)$ and let $\iota_H : H \to G \times H$ be given by $\iota_H(h) = (1, h)$. Clearly ι_G, ι_H are injective group homomorphisms. Define

$\varphi : (G \times H)^\vee \to G^\vee \times H^\vee$ by $\varphi(\chi) = (\chi \circ \iota_G, \chi \circ \iota_H)$. Define $\phi : G^\vee \times H^\vee \to (G \times H)^\vee$ by $\phi(\chi_1, \chi_2)(g, h) = \chi_1(g)\chi_2(h)$. The reader may then check that φ, ϕ are well-defined and are inverses of each other. Hence, (3).

Since G is finite and abelian, it is non-canonically isomorphic to the direct product of cyclic groups, so we may write $G \simeq \prod_{i=1}^n \mathbb{Z}/a_i\mathbb{Z}$ with, when G is nontrivial, all $a_i > 1$.

Note. Here, unlike above, we are taking the group operation of the right hand side to be (component-wise) addition.

Then, by (3), $G^\vee \simeq \prod_{i=1}^n (\mathbb{Z}/a_i\mathbb{Z})^\vee$. So it suffices to consider $\mathbb{Z}/a\mathbb{Z}^\vee$ for $a > 1$. Recall from above that $1 = \chi(g)^a$, so we pick a generator g of $\mathbb{Z}/a\mathbb{Z}$ and associate it to $e^{2\pi i/a}$. This is why the isomorphism will be non-canonical. Then, since the ath roots of unity are a cyclic group of order a, there is a (again non-canonical) map into $\mathbb{Z}/a\mathbb{Z}$. Composing the aforementioned then yields an isomorphism of $(\mathbb{Z}/a\mathbb{Z})^\vee$ and $\mathbb{Z}/a\mathbb{Z}$ By the prefacing remark, hence (1).

Finally, let $\widehat{\ }: G^\vee \to \mathbb{C}^*$ be the evaluation map, i.e. $\widehat{g} : \chi \mapsto \chi(g)$ and $\widehat{\ }: g \mapsto \widehat{g}$. The reader can easily check that $\widehat{\ }$ is an injective group homomorphism and so since, by (1), $|G| = |G^\vee| < \infty$, also surjective. Hence (2). □

Lemma 2.3. *Let $\mathbb{C}(G)$ be the vector space of complex-valued functions on a finite abelian group G, equipped with inner product $\langle f_1, f_2 \rangle = |G|^{-1} \sum_{g \in G} f_1(g)\overline{f_2(g)}$. Then,*

1. *The $\chi \in G^\vee$ form a basis of $\mathbb{C}(G)$.*
2. *This basis is orthonormal with respect to $\langle , \rangle$.*

Proof. As shown in the proof of 2.2, $\chi(g)$ is always a root of unity, and so, in particular, $1 = |\chi(g)|^2 = \chi(g)\overline{\chi(g)}$, and thus $\chi(g)^{-1} = \overline{\chi(g)}$. We may then compute,

$$\langle \chi, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi(g)} = \frac{1}{|G|} \sum_{g \in G} \chi(g)\chi(g)^{-1} = \frac{1}{|G|} \sum_{g \in G} \chi(gg^{-1}) = 1$$

Next, consider $\sum_{g \in G} \chi(g)$. For $\chi \neq 1$, there exists some $h \in G$ such that $\chi(h) \neq 1$. Since $g \mapsto hg$ is a bijection,

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(g)$$

Since $\chi(h) \neq 1$, we have $\sum_{g \in G} \chi(g) = 0$, and

$$|G|\langle \chi, 1 \rangle = \sum_{g \in G} \chi(g) = 0$$

Thus, $\langle \chi, 1 \rangle = 0$ for $\chi \neq 1$. Then,

$$|G|\langle \chi_1, \chi_2 \rangle = \sum_{g \in G} \chi_1(g)\overline{\chi_2(g)} = \sum_{g \in G} \chi_1(g)\chi_2^{-1}(g) = \sum_{g \in G} (\chi_1\chi_2^{-1})(g) = |G|\langle \chi_1\chi_2^{-1}, 1 \rangle$$

Which is 0 if and only if $\chi_1\chi_2^{-1} \neq 1$ if and only if $\chi_1 \neq \chi_2$. Hence (2).

For (1), we may recall from linear algebra that $\dim \mathbb{C}(G) = |G|$ and that orthogonal sets are linearly independent. By 2.2, $|G| = |G^\vee|$, so $G^\vee$ is a linearly independent set with the correct size. Hence (1). □

Fix $\{\lambda_n\} \subseteq \mathbb{R}_{>0}$ such that $\lambda_n \to \infty$. We will usually take $\lambda_n = \log n$.

Definition. A Dirichlet series is a series of the form $\sum_{n=1}^{\infty} a_n e^{-\lambda_n z}$, where $a_n \in \mathbb{C}$.

Next time. We will examine the convergence and analytical properties of Dirichlet series, prove the first and second parts of 2.3, and apply these results to L-functions.