MAT417 Lecture Notes

Isaac Clark

September 20, 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):

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

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

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

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

Remark. 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.

Nomenclature. Going forward, when unambiguous, I will use character to refer to both group characters and Dirichlet characters despite the latter technically being an arithmetic function, and trust the reader to infer which is correct. I will also use χ to denote either if only one or the other makes an appearance.

Definition. For a fixed 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 group 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, homomorphisms, 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 $e^{2\pi i/a}$. Then, since the ath roots of unity are a cyclic group of order a, there is a (again non-canonical) isomorphism into $\mathbb{Z}/a\mathbb{Z}$. Composing these 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 $\widehat{\ }\colon G^\vee \to \mathbb{C}^*$ be the evaluation map, i.e. $\widehat{g} : \chi \mapsto \chi(g)$ and $\widehat{\ }\colon g \mapsto \widehat{g}$. The reader can easily check that $\widehat{\ }$ is an injective group homomorphism and so since, by (1), $|G| = |G^\vee| < \infty$, also surjective. This association is canonical. 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 **Theorem 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).

Finally, we recall from linear algebra that $\dim \mathbb{C}(G) = |G|$ and that orthogonal sets are linearly independent. By **Theorem 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 **Theorem 2.3**, and apply these results to L-functions.

3 Weeks 2, 3 - Dirichlet's theorem and Quadratic reciprocity

3.1 Towards Dirichlet's theorem

At this point, as I am behind on the notes I have the benefit of hindsight, and so will deviate from Lawrence's notes to give a more streamlined approach to the material covered in Weeks 2 and 3. Fix $m \in \mathbb{Z}^+$. Organizationally, we will prove an extension of **Theorem 2.3** as the following theorems.

Theorem 3.1. *Let χ be a character of $(\mathbb{Z}/m\mathbb{Z})^*$. Then,*

1. *$L(\chi, s)$ is holomorphic for $\mathfrak{Re}(s) > 1$.*
2. *$L(\chi, s)$ extends meromorphically to $\mathfrak{Re}(s) > 0$.*
3. *For $\chi \neq 1$, $L(\chi, s)$ is holomorphic for $\mathfrak{Re}(s) > 0$ and the series converges.*
4. *If $\chi = 1$, then $L(\chi, s)$ has only a simple pole at $s = 1$.*

Theorem 3.2. *If $\chi \neq 1$, then $L(\chi, 1) \neq 0$.*

We will see (much) later that these theorems imply Dirichlet's theorem on primes in arithmetic progressions. The following prepatory theorems were largely stated without proof in lecture, so I've supplied them, which means that there is a large probability of them having mistakes, let me know if you find any.

Lemma 3.1. *Suppose $\{f_n(z)\}$ is a sequence of holomorphic functions on some domain $U \subseteq \mathbb{C}$. Suppose also that there is a function $f(z)$ on U such that $\lim_{n\to\infty} f_n(z) = f(z)$ for all $z \in U$ and that this convergence is uniform on compact subsets of U. Then $f(z)$ is holomorphic and $f'(z) = \lim_{n\to\infty} f_n'(z)$.*

Proof. Hard complex analysis. Come back later. □

Lemma 3.2. *Let $\{a_n\}_{n\in\mathbb{N}}, \{b_n\}_{n\in\mathbb{N}}$ be sequences in $\mathbb{C}$. Put $A_{m,k} = \sum_{n=m}^{k} a_n$ and $S_{m,k} = \sum_{n=m}^{k} a_n b_n$. Then, $S_{m,m'} = \sum_{n=m}^{m'-1} A_{m,n}(b_n - b_{n+1}) + A_{m,m'} b_{m'}$.*

Proof. Write $a_n = A_{m,n} - A_{m,n-1}$ and then rearrange terms. □

Lemma 3.3. *Suppose $0 < \alpha < \beta$, $z \in \mathbb{C}$ with $\mathfrak{Re}(z) > 0$. Write $z = x + iy$. Then,*

$$\left|e^{-\alpha z} - e^{-\beta z}\right| \leq \frac{|z|}{x}\left(e^{-\alpha x} - e^{-\beta x}\right)$$

Proof. Observe that, $z\int_\alpha^\beta e^{-tz}\, dt = e^{-\alpha z} - e^{-\beta z}$. And so,

$$|e^{-\alpha t} - e^{-\beta z}| \leq |z| \int_\alpha^\beta |e^{-tz}|\, dt = |z| \int_\alpha^\beta e^{-tx}\, dt = \frac{|z|}{x}(e^{-\alpha x} - e^{-\beta x})$$

It may be a good exercise to show that $|e^{-tz}| = e^{-tx}$ as a sanity check. □

Theorem 3.3. *Suppose $f(z) = \sum_{n=0}^{\infty} a_n e^{-\lambda_n z}$ converges for some $z = z_0$. Then it is uniformly convergent on every sector of z_0, i.e. every set of the form*

$$\{z \in \mathbb{C} \mid |Arg(z - z_0)| \leq \alpha < \pi/2\}$$

Proof. We may assume without loss of generality that $z_0 = 0$. Suppose $z \in \mathbb{C}$ is such that $\mathrm{Arg}(z) > 0$. In particular, $\mathfrak{Re}(z) > 0$. Then, $f(0) = \sum_{n=0}^{\infty} a_n$ converges, and so the $A_{m,k} = \sum_{n=m}^{k} a_n$ can be made small. Put $S_{m,k} = \sum_{n=m}^{k} a_n e^{-\lambda_n z}$. Write $z = x + iy$. Fix $\varepsilon > 0$. Since $\lambda_n \to \infty$ as $n \to \infty$, $x > 0$, and $e^{-t} \to 0$ as $t \to \infty$, we can pick N such that $e^{-\lambda_n x} < \varepsilon x |z|^{-1}$ for $n \geq N$. Take $m \geq N$ large enough that we also have $|A_{m,n}| < \varepsilon$ for all $n \geq m$, write $z = x + iy$ with $x > 0$, and take k larger than m. We

then estimate,

$$\begin{aligned}
|S_{m,k}| &= \left| \sum_{n=m}^{k-1} A_{m,n}(e^{-\lambda_n z} - e^{-\lambda_{n+1} z}) + A_{m,k} e^{-\lambda_k z} \right| \text{ , by } \textbf{Lemma 3.2} \\
&\leq \sum_{n=m}^{k-1} |A_{m,n}| \cdot \left| e^{-\lambda_n z} - e^{-\lambda_{n+1} z} \right| + |A_{m,k}| \cdot \left| e^{-\lambda_k z} \right| \\
&\leq \varepsilon \left(\frac{|z|}{x} \sum_{n=m}^{k-1} \left| e^{-\lambda_n x} - e^{-\lambda_{n+1} x} \right| \right) + \varepsilon \left| e^{-\lambda_k x} \right| \text{ , by } \textbf{Lemma 3.3} \\
&\leq \varepsilon \frac{|z|}{x} \left(\sum_{n=m}^{k-1} e^{-\lambda_n x} - e^{-\lambda_{n+1} x} \right) + \varepsilon^2 \frac{x}{|z|} \text{ , since the } \lambda_n \text{ are strictly increasing} \\
&= \varepsilon \frac{|z|}{x} \left(e^{-\lambda_m x} - e^{-\lambda_k x} \right) + \varepsilon^2 \frac{x}{|z|} \\
&\leq 3\varepsilon^2
\end{aligned}$$

And so $f(z)$ converges uniformly. □

Corollary 3.1. (**Theorem 3.3** + **Lemma 3.1**) $\implies$ (1) of **Theorem 3.1**.

Proof. Fix $z_0 \in \mathbb{C}$ with $\mathfrak{Re}(z_0) > 1$. Then by **Theorem 2.2**, $L(\chi, z_0)$ converges. Put $U = \{z \in \mathbb{C} \mid \mathfrak{Re}(z) > \mathfrak{Re}(z_0)\}$. Since the sectors form an open cover of the half plane $\{z \in \mathbb{C} \mid \mathfrak{Re}(z) > \mathfrak{Re}(z_0)\}$, every compact subset of U can be covered by finitely many sectors. On each sector, by **Theorem 3.3**, $L(\chi, s)$ converges uniformly, and so $L(\chi, s)$ converges uniformly on any compact subset of U. By **Lemma 3.1** and taking $z_0 = 1 + \varepsilon$ and sending $\varepsilon \to 0^+$, we have that $L(\chi, s)$ is holomorphic on $\mathfrak{Re}(z) > 1$. □

For part of (2) and (4) of **Theorem 3.1**, consider that $L(1, s) = \zeta(s) \prod_{p|m}(1 - p^{-s})$. The $\prod_{p|m}(1 - p^{-s})$ piece clearly does not vanish at $s = 1$. So it suffices to show that $\zeta(s)$ is meromorphic for $\mathfrak{Re}(s) > 0$ and has a unique simple pole at $s = 1$. In particular, we will show that $\zeta(s) = (s-1)^{-1} + \varphi(s)$ where $\varphi(s)$ is holomorphic on $\mathfrak{Re}(s) > 0$.

Definition. For a sequence $\{\varphi_n\}_{n \in \mathbb{N}}$ of functions on some domain, we say that $\sum_n \varphi_n$ converges normally if $\sum_n \sup_s |\varphi_n(s)|$ converges.

Theorem 3.4. *Normal convergence implies uniform absolute convergence.*

Proof. Come back to this later. □

For $\mathfrak{Re}(s) > 1$, $(s-1)^{-1} = \int_1^\infty t^{-s}\, dt = \sum_n \int_n^{n+1} t^{-s}\, dt$. So, for $\mathfrak{Re}(s) > 1$,

$$\zeta(s) = \frac{1}{s-1} + \sum_n \int_n^{n+1} n^{-s} - t^{-s}\, dt$$

Put $\varphi_n(s) = \int_n^{n+1} n^{-s} - t^{-s}\, dt$. We estimate,

$$\begin{aligned}
\sup_s |\varphi_n(s)| &\leq \sup_{n \leq t \leq n+1} |n^{-s} - t^{-s}| \\
&\leq \sup_{n \leq t \leq n+1} \left| \frac{d}{dt} t^{-s} \right| \text{ , by the mean value theorem} \\
&= \sup_{n \leq t \leq n+1} \left| \frac{s}{t^{s+1}} \right| \\
&\leq \frac{|s|}{n^{\mathfrak{Re}(s)+1}}
\end{aligned}$$

Then, if $\mathfrak{Re}(s) \geq \varepsilon$, then $\sum_n \sup_s |\varphi_n(s)| \leq \sum_n |s| n^{-1-x}$ converges and so we have uniform absolute convergence and thus that $\varphi(s) = \sum_n \varphi_n(s)$ is holomorphic for $\mathfrak{Re}(s) > 0$. Thus, $\zeta(s) = (s-1)^{-1} + \varphi(s)$ is a meromorphic extension of ζ to $\mathfrak{Re}(s) > 0$ with only a simple pole at $s = 1$. With this we have, by the above remarks, that $L(1, s)$ extends meromorphically to $\mathfrak{Re}(s) > 0$ with only a simple pole at $s = 1$, and thus we have (4) and the case where $\chi = 1$ of (2) of **Theorem 3.1**. With this it is also now possible to make sense of the Riemann hypothesis.

Riemann Hypothesis. For $\mathfrak{Re}(s) > 0$, the only zeroes of $\zeta(s)$ have $\mathfrak{Re}(s) = 1/2$.

We move now to prove **Theorem 3.1** for $\chi \neq 1$. If $L(\chi, s)$ converges for $\mathfrak{Re}(s) > 0$ then, by the same argument as in the proof of **Corollary 3.1**, we would have that $L(\chi, s)$ is holomorphic on $\mathfrak{Re}(s) > 0$.

Lemma 3.4. *Suppose $\sum_n a_n n^{-s}$ is a Dirichlet series such that all partial sums of the a_n are bounded. Then $\sum_n a_n n^{-s}$ converges for $\mathfrak{Re}(s) > 1$.*

Proof. Let $A_{k,k'} = \sum_n = k^{k'} a_n$. Pick K such that $|A_{k,k'}| < K$ for all k, k'. Let $S_{k,k'} = \sum_{n=k}^{k'} a_n n^{-s}$. Then, for $x = \mathfrak{Re}(s) > 0$,

$$
\begin{aligned}
|S_{k,k'}| &\leq K\left(\sum_{n=k}^{k'-1}\left|n^{-s}-(n+1)^{-s}\right|\right)+\left|(k')^{-s}\right| \text{ , by } \textbf{Lemma 3.2} \\
&\leq K\left(\sum_{n=k}^{k'-1} n^{-x}-(n+1)^{-x}\right)+\left|(k')^{-x}\right| \text{ , by } \textbf{Lemma 3.3} \\
&= K(k^{-x}-(k')^{-x})+(k')^{-x} \\
&\leq Kk^{-x}+(k')^{-x}
\end{aligned}
$$

Which can each be made arbitrarily small for k, k' sufficently large. □

Corollary 3.2. For $\chi \neq 1$, by **Lemma 2.3** we have, for all k,

$$\sum_{n=k}^{k+m-1}\chi(n)=\sum_{a\in(\mathbb{Z}/m\mathbb{Z})^*}\chi(a)=0$$

So the $A_{k,k'}=\sum_{n=k}^{k'}\chi(n)$ can take only finitely many values, in paritcular, the values for $k'-k<m$ and $k\leq m$. Thus all of the parital sums are bounded, and so by **Lemma 3.4** we have that $L(\chi,s)$ converges on $\mathfrak{Re}(s)>0$, and so by the above remark, that it is holomorphic on $\mathfrak{Re}(s)>0$. Hence (3) of **Theorem 3.1**.

Define $\zeta_m(s)=\prod_\chi L(\chi,s)$ to be the product over all characters χ of $(\mathbb{Z}/m\mathbb{Z})^*$ of their corresponding L-functions. By (2) and (3) of **Theorem 3.1** we have that ζ_m is meromorphic on $\mathfrak{Re}(s)>0$.

Digression. A central notion from algebraic number theory is that of a number field, i.e. a finite extension of $\mathbb{Q}$. Then, with the proper machinery (consider taking 415 if you're interested) we can define functions on number fields with similar analytical properties to $\zeta(s)$. It turns out, if $\zeta_K(s)$ denotes the "zeta function" for a number field K, then $\zeta_{\mathbb{Q}}(s)=\zeta(s)$ and for K a cyclotomic extension of order m, then $\zeta_K(s)=\zeta_m(s)$.

If p is a prime such that $p\nmid m$ then $(p,m)=1$ and so $\overline{p}\in(\mathbb{Z}/m\mathbb{Z})^*$. Let $f(p)$ be the order of $\overline{p}$ in $(\mathbb{Z}/m\mathbb{Z})^*$. Let $g(p)=\varphi(p)/f(p)$. Since $f(p)\mid\varphi(p)$, $g(p)$ is an integer.

Lemma 3.5. *Let A be a finite abelian group. Let $B\leq A$ be a subgroup. Let χ_B be a character on B. Then there are exactly $|A/B|$ extensions of χ_B to A.*

Proof. For any G, H groups and $\phi: G\to H$ homomorphism, ϕ naturally induces a map $H^\vee\to G^\vee$ given by $\chi\mapsto\chi\circ\phi$. One can check that this association is a contravariant functor from groups to their duals. Consider the short exact sequence,

$$0\to B\xrightarrow{\iota}A\xrightarrow{\pi}A/B\to 0$$

Since contravariant functors take injections to surjections and vice versa, we get another short exact sequence,

$$0 \to (A/B)^\vee \xrightarrow{\pi^*} A^\vee \xrightarrow{\iota^*} B^\vee \to 0$$

By the universal property of the quotient group, it follows that $B^\vee \cong A^\vee/(A/B)^\vee$. For $\chi \in A^\vee$, $\iota^*\chi = \chi \circ \iota$, so ι^* is simply the restriction map. Taken together, for any χ_B character of B, $(\iota^*)^{-1}(\chi_B)$, the characters on A which restrict to χ_B, can be uniquely associated to a coset in $A^\vee/(A/B)^\vee$, which has cardinality $|A/B|$. □

Let T be a free variable. Since $\prod_{\omega^n=1}(1-\omega T) = (1-T)^n$, for fixed $p \nmid m$ we have that $\prod_\chi (1-\chi(p)T) = (1-T^{f(p)})^{g(p)}$ since $\chi(p)^{f(p)} = 1$ by definition and there are exactly $g(p)$ characters such that $\chi(p) = \omega$ for each ω an $f(p)$-th root of unit, per **Lemma 3.5**.

Thus, we may write,

$$\zeta_m(s) = \prod_{p \nmid m} \left(1 - p^{-f(p)s}\right)^{-g(p)} = \prod_{p \nmid m} \left(\sum_{k=0}^{\infty} p^{-kf(p)s}\right)^{g(p)}$$

Expanding, we'll get a Dirichlet series of the form $\sum_n a_n n^{-s}$, where the $a_n \geq 0$.

Lemma 3.6. *Suppose $f(z) = \sum_n a_n e^{-\lambda_n z}$ for λ_n an increasing, positive sequence of real numbers which tends to ∞ as $n \to \infty$. Suppose further that $a_n \geq 0$, that there exists some $\rho \in \mathbb{R}$ such that $f(z)$ converges for $\mathfrak{Re}(z) > \rho$, and that f analytically continues to a neighbourhood of ρ. Then, there exists some $\varepsilon > 0$ such that $f(z)$ converges for $\mathfrak{Re}(z) > \rho - \varepsilon$.*

Proof. In Serre. Come back to this later. □

Corollary 3.3. If $\zeta_m(s)$ has no pole at $s = 1$, then by **Lemma 3.6** $\zeta_m(s)$ would converge on $\mathfrak{Re}(z) > 0$. Since $f(p) \leq \varphi(p)$, we have that $\prod_{p \nmid m} \sum_{k=0}^{\infty} p^{-k\varphi(m)s}$ converges for $\mathfrak{Re}(z) > 0$. But then $\prod_p \sum_{k=0}^{\infty} p^{-k\varphi(m)s} = \sum_{n=1}^{\infty} n^{-\varphi(m)s}$ only differs from the former by finitely many terms, and so it converges. However, this series certainly diverges for $s = \varphi(m)^{-1}$. Thus, $\zeta_m(s)$ has a pole at $s = 1$. By (3) of **Theorem 3.1**, each $L(\chi, s)$, for $\chi \neq 1$, converges for $s = 1$, so in particular none of them have poles at $s = 1$. This means that there's no "funny business" with some of the $L(\chi, s)$ vanishing at $s = 1$ and some having poles at $s = 1$, and with **Lemma 3.6** we really do have that none of the $L(\chi, 1)$ vanish at $s = 1$. Hence (2) of **Theorem 3.2**.

3.2 Density, Dirichlet's theorem

Lemma 3.7. *For $s > 1$, $\sum_p p^{-s} = -\log(s-1) + O(1)$ as $s \to 1^+$.*

Proof. As shown in the proof of (3) of **Theorem 3.1**, $\zeta(s)$ has a simple pole at $s = 1$. Thus we can write $\log(\zeta(s)) = -\log(s-1) + O(1)$ for $s > 1$. But

$$\log(\zeta(s)) = \sum_p \log\left((1-p^{-s})\right) = \sum_{k=1}^{\infty}\sum_p \frac{1}{kp^{ks}}$$

So it suffices to show that the above sum remains bounded as $s \to 1^+$. But this is clear, since

$$\sum_{k=2}^{\infty}\sum_p \frac{1}{kp^{ks}} \leq \sum_p \frac{1}{p^s(p^s-1)} \leq \sum_p \frac{1}{p(p-1)} < \zeta(2)$$

And so we have the claim. □

Definition. Let P be the set of all primes. We say that $A \subseteq P$ has density k if $\lim_{s\to 1^+} -\log(s-1)^{-1}\sum_{p\in A} p^{-s} = k$. By **Lemma 3.7**, this definition makes sense for any $A \subseteq P$, and $0 \leq k \leq 1$. Clearly, if $k > 0$ then $|A| = \infty$.

Remark. We say that $A \subseteq B \subseteq \mathbb{N}$ has natural density k in B if

$$\lim_{n\to\infty} \frac{|A \cap [0,n]|}{|B \cap [0,n]|} = k$$

If $A \subset P$ has natural density k in P, then A has density k. But the converse is not true in general. Dirichlet's theorem is true if, in the below formulation, we replace density with natural density, though we won't prove this (stronger) version.

Theorem 3.5. *For $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$ with $(a,m) = 1$, let P_a be the set of primes which are congruent to $a \mod m$. Then P_a has density $\varphi(m)^{-1}$. In particular, there are infinitely many primes which are congurent to a mod m.*

Proof. We will break this down into 4 steps.

(S1) Since there are only finitely many primes which divide m, by **Lemma 3.7**, $L(1,s) \sim -\log(s-1)$.

(S2) Suppose $\chi \neq 1$. Then

$$\log(L(\chi,s)) = \sum_{p\nmid m}\sum_{k=1}^{\infty} \frac{\chi(p)^k}{kp^{ks}} = L(\chi,s) + \sum_p \sum_{k=2}^{\infty} \frac{\chi(p)^k}{kp^{ks}}$$

Further,

$$\left|\sum_p \sum_{k=2}^{\infty} \frac{\chi(p)^k}{kp^{ks}}\right| \leq \sum_p \sum_{k=2}^{\infty} \frac{1}{kp^{ks}}$$

So this term is bounded as $s \to 1$. Since, by **Theorem 3.2**, $L(\chi, 1) \neq 0$, we also have that $\log(L(\chi, s))$ is bounded as $s \to 1$. Taken all together, $L(\chi, s)$ is also bounded as $s \to 1$.

(S3) Let $g_a(s) = \sum_{p \in P_a} p^{-s}$. Then,

$$\sum_{\chi} \chi(a)^{-1} L(\chi, s) = \sum_{\chi} \sum_{p \nmid m} \chi(a)^{-1} \chi(p) p^{-s} = \sum_{p \nmid m} \sum_{\chi} \chi(a^{-1}p) p^{-s}$$

But we also have that $\sum_{\chi} \chi(a^{-1}p) = \varphi(m)$ if $a^{-1}p \equiv 1 \mod m$ and 0 otherwise. So,

$$\sum_{\chi} \chi(a)^{-1} L(\chi, s) = \varphi(m) g_a(s)$$

(S4) By (S1) and (S2), $\lim_{s \to 1^+} -\log(s-1)^{-1} L(\chi, s) = 1$ if $\chi = 1$ and 0 otherwise. Finally, applying this with (S3), we have

$$\lim_{s \to 1^+} \frac{-g_a(s)}{\log(s-1)} = \lim_{s \to 1^+} \frac{-\sum_{\chi} \chi(a)^{-1} L(\chi, 1)}{\varphi(m) \log(s-1)} = \frac{1}{\varphi(m)} \sum_{\chi} \chi(a)^{-1} \lim_{s \to 1^+} \frac{-L(\chi, s)}{\log(s-1)} = \frac{1}{\varphi(m)}$$

Which finishes the proof. And thus our first big theorem of the course. □

3.3 Quadratic reciprocity, finite fields

Moving on, let $a \in \mathbb{Z}$. We will now explore quadratic reciprocity. For p prime, we define $\left(\frac{a}{p}\right)$ to be 0 if $p \mid a$, 1 if $p \nmid a$ and a is a square mod p, and -1 if $p \nmid a$ and a is not a square mod p. If we fix p, the Legendre symbol is multiplicative.

Theorem 3.6. *If p, q prime, n an odd integer. Put $\varepsilon(n) = (n-1)/2 \mod 2$. Then,*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\varepsilon(p)\varepsilon(q)}$$

Proof. Elementary number theory. Come back later. □

Theorem 3.7. *Suppose $a \in \mathbb{Z}$ is nonzero and square-free. Let $m = 4|a|$. Then there exists a unique character χ_a on $(\mathbb{Z}/m\mathbb{Z})^*$ such that $\chi_a(p) = \left(\frac{a}{p}\right)$ for all $p \nmid m$.*

Proof. In Serre Chapter 1, by quadratic reciprocity apparently. Come back later. □

Theorem 3.8. *For $a \in \mathbb{Z}$ not a square, the set of p such that $\left(\frac{a}{p}\right) = 1$ has density $1/2$.*

Proof. We can assume without loss of generality that a is square-free. Let $m = 4|a|$. Let χ_a be the character as in **Theorem 3.7**. Let $H \subseteq (\mathbb{Z}/m\mathbb{Z})^*$ be its kernel. For $p \nmid m$, $\chi_a(p) = 1$ if and only if $p \in H$. In particular, $|H| = \varphi(m)/2$. For any $x \in (\mathbb{Z}/m\mathbb{Z})^*$ the density of primes p such that $p \equiv x \mod m$ is, by **Theorem 3.5**, $\varphi(m)^{-1}$. And so, taken all together, the density of p such that $p \in H$ is $1/2$. □

Corollary 3.4. If the set of all primes p such that $\left(\frac{a}{p}\right) = 1$ has density greater than $1/2$, then a must be a square.

Fix a prime p, then $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field. We recall that for any field K, either $n \cdot 1_K \neq 0$ for all $n \in \mathbb{Z}$, in which case we say that K has characteristic 0, or there is a prime p such that $\{n \in \mathbb{Z} \ : \ n \cdot 1_K = 0\} = (p)$, and we say that K has characteristic p. If K is finite, then the map $\mathbb{Z} \to K$ given by $n \mapsto n \cdot 1_K$ cannot be injective, and so K has non-zero characteristic. In particular, this map is a homomorphism, and so its image is a unital subring of K, and thus isomorphic to $\mathbb{F}_p$ for some prime p. Then K is a finite-dimensional vector space over this "copy" of $\mathbb{F}_p$ and so has cardinality p^n for some $n \geq 1$. So finite fields must have prime power cardinality. Conversely, we claim that given p prime and $n \geq 1$, there is a unique (up to isomorphism) field of cardinality $q = p^n$. Let $K = \overline{\mathbb{F}_p}$ be the algebraic closure of $\mathbb{F}_p$, which is unique up to isomorphism. One can check via the binomial theorem that the map $x \mapsto x^q$ is a ring homomorphism. Consider $\mathbb{F}_q = \{x \in K \ : \ x^q = x\}$, by the aforementioned remark, this is a subfield of K. Since K is algebraically closed, $\mathbb{F}_q$ contains at most q distinct elements, as every polynomial of degree q in K has, counting multiplicity, q roots. On the other hand, the formal derivative of $x^q - x$ is simply -1, and so the greatest common divisor of $x^q - x$ and its derivative is 1, and so there are no repeated roots, and so there are precisely q elements in $\mathbb{F}_q$. For uniqueness, if L is a field with q elements, its multiplicative group L^* has size $q - 1$, so $x^{q-1} = 1$ for every $x \neq 0$ in L, and thus $x^q = x$ for all $x \in L$. Since L can naturally be embedded in K and consists of all roots of $x^q - x$ in K, we have uniqueness up to isomorphism.

Lemma 3.8. *Suppose $n \geq 1$, then $\sum_{d|n} \varphi(d) = n$.*

Proof. Come back later. □

Lemma 3.9. *Let H be a finite group of order n. Suppose that for all $d \mid n$ we have $|\{x \in H \ : \ x^d = 1\}| \leq d$. Then H is cyclic.*

Proof. If $x \in H$ has order d, then $|\langle x \rangle| = d$. And so, for all $y \in H$ such that $y^d = 1$, it must be that $y = x^i$ for some i, as $d = |\langle x \rangle| \leq |\{h \in H \ : \ h^d = 1\}| \leq d$. Thus, there are $\varphi(d)$ elements of order d in H, in paritcular, the elements of the form x^i for i coprime to d. Then, by **Lemma 3.8**, $|H| = \sum_{d|n} \varphi(d)$. By our previous calculation, if there

is an element of order d then there are precisely $\varphi(d)$ elements of order d. Further, since every element of H has an order dividing d, $|H| = \sum_{d|n} |\{h \in H \ : \ \text{ord}(h) = d\}|$. Where each $|\{h \in H \ : \ \text{ord}(h) = d\}|$ is either $\varphi(d)$ or 0. Thus, each is non-empty, and so in particular there exists an element of order n in H, and so H is cyclic. □

Theorem 3.9. *For all $q = p^n$, $\mathbb{F}_q^*$ is cyclic.*

Proof. First, $|\mathbb{F}_q^*| = q-1$. Then, for all $d \mid (q-1)$, $\{x \in \mathbb{F}_q^* \ : \ x^d = 1\}$ are precisely the roots of $x^d - 1$ in $\mathbb{F}_q$, of which there are at most d. Thus, the premise of **Lemma 3.9** is satisfied, and so we have the claim. □

Corollary 3.5. If $p \nmid a$ for p an odd prime, then $\left(\frac{a}{p}\right) = a^{(p-1)/2} \mod p$.

Proof. By Fermat's little theorem, $a^{p-1} \equiv 1 \mod p$. So $a^{(p-1)/2}$ is conrguent to either 1 or -1 mod p. If $a = b^2$, then $a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \mod p$. Conversely, since $\mathbb{F}_p^*$ is cyclic of even order, if $a^{(p-1)/2} = 1$ then there is an element $b \in \mathbb{F}_p^*$ such that $a = b^2$. □

Lemma 3.10. *Let p an odd prime. Then,*

1. $\left(\frac{1}{p}\right) = 1$.
2. $\left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$.
3. $\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$.
4. $\left(\frac{p}{2}\right) = 1$.

Where $\omega(n) = (n^2-1)/8 \mod 2$, for n an odd integer.

Proof. Come back later. □