MAT417 Lecture Notes

Arky!! :3c

'25 Fall Semester

Contents

§1 Day 1: Course Administrative Details and Preliminaries (Sep. 2, 2025)

Course materials will be free and available online; here is a list of reference materials:

- Serre's *Course in Arithmetics* up to Chapter 4,
- Lecture notes by Noam Elkies (which will be posted on Quercus).

Homework will be posted every Thursday and due the following Thursday, and is worth **20%** of the course grade.

The central question of number theory is about the structure of prime numbers, of which the main analytic tools used are the Riemann ζ-functions and its relatives (the L-functions). We may discuss things like modular forms, Hecke operators and L-functions related to Galois representation later on.

Let us consider the following two questions;

(a) How many primes are there? There are infinitely many of them.

(b) Can you say something about how the primes are distributed?

Given $x > 0$, where x may be a natural or a real, let us define

$$\pi(x) = \#\{p \text{ is prime} \mid p \leq x\}.$$

Can we estimate how $\pi(x)$ grows? The prime number theorem states that the growth of $\pi(x)$ is proportional to $\frac{x}{\log x}$, i.e.,

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1, \qquad \frac{\pi(x)}{x} \to 0 \text{ as } x \to \infty.$$

As an exercise, show that the prime number theorem informally says that the nth prime p_n is of the size $n \log n$.

Theorem 1.1 (Dirichlet Theorem)**.** Let a, d be coprime naturals where $a < d$. Consider all numbers of the form $a + kd$, where k is also a natural; infinitely many of these numbers are prime.

Proof. Done with L-functions. Check here. $\square$

Theorem 1.2 (Fundamental Theorem of Arithmetic)**.** Any nautral number N can be written uniquely as $p_1^{a_1} \dots p_n^{a_n}$, where p_i are primes and $a_i > 0$.

Proposition 1.3 (Euclid's Argument on the Infinitude of Primes)**.** Assume that $p_1 < p_2 < \cdots < p_n$ constitute all the primes. Then it is clear that $p_1 \dots p_n + 1$ is coprime to any p_i. By the fundamental theorem of arithmetic, this means that $p_1 \dots p_n + 1$ is divisible by a prime less than $p_1 \dots p_n + 1$ not given by some p_i, which is a contradiction.

Can we use this to get an estimate on $\pi(x)$? We claim that $\pi(x) > \log_2 \log_2 x$. Let p_n be the nth prime. Then

$$p_{n+1} < 1 + \prod_{i=1}^{n} p_i < \prod_{i=1}^{n} p_n.$$

If equality always held then we would have $p_n = 2^{2^{n-1}}$. However, in actuality, $p_n < 2^{2^{n-1}}$, so we must have that $\pi(x) > \log_2 \log_2 x$.

The Riemann-Zeta function is given by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Claim 1.4. ζ is absolutely convergent for any $s > 1$.

Proof. Will be given next class. $\square$

Lemma 1.5. For $s > 1$, we have that

$$\zeta(s) \leq \prod_{p \text{ is prime}} \frac{1}{1 - p^{-s}}.$$

Proof. This is given directly by geometric series, i.e.,

$$\frac{1}{1 - p^{-s}} = \sum_{i=0}^{\infty} p^{-is} = \sum_{\substack{p_1 < \cdots < p_n \\ a_1, \ldots, a_n > 0}} p_1^{a_1} \ldots p_n^{a_n}. \qquad \square$$

Moreover, if we had finitely many primes, we could apply this to $s = 1$ and obtain that the sum of $\frac{1}{n}$ is convergent, which is clearly false. This also implies that the sum of the reciprocals of primes is divergent, and you can't have $\pi(x)$ be bounded from above by Cx^D, where $C > 0, D < 1$.

§2 Day 2: More accurate treatment of the Riemann-Zeta function (Sep. 4, 2025)

Note that I won't be here for the second hour of Thursday classes because I have complex analysis during that time. Isaac will be taking the full hour's worth of notes, though. *i lied i'm staying for this lecture*

Today's lesson agenda is as follows,

(i) More accurate treatment of $\zeta(s)$;

(ii) Prove that $\sum_{p \text{ is prime}} \frac{1}{p}$ is divergent (per Euler),

(iii) Start doing preaptory material for the Dirichlet theorem, and introduce the Dirichlet L-functions.

Lemma 2.1. The Riemann-Zeta function is convergent for $s \in \mathbb{R}$, $s > 1$; it is absolutely convergent for $s \in \mathbb{C}$, $\Re s > 1$.

We will later prove that for $\Re s > 1$, $\zeta(s)$ is a holomorphic function. Let's start by comparing $\sum \frac{1}{n^s}$ to $\int_1^\infty x^{-s}\,dx$; observe that

$$\int_1^a x^{-s}\,dx = \frac{x^{1-s}}{1-s}\bigg|_1^a = \frac{a^{1-s}}{1-s} - \frac{1}{1-s},$$

of which a^{1-s} approaches 0 as $a \to \infty$. Thus, we have that

$$\int_1^\infty x^{-s} = \frac{1}{s-1}.$$

We also have that

$$\sum_{n=2}^{\infty} n^{-s} \le \int_1^\infty x^{-s}\,dx = \frac{1}{s-1},$$

and

$$\sum_{n=2}^{N} n^{-s} \le \int_1^N x^{-s}\,dx,$$

which yields convergence. Thus, we have that inequality that $\zeta(s) \le 1 + \frac{1}{s-1}$.

Exercise 2.2. Run a very similar argument and prove that $\zeta(s) > \frac{1}{s-1}$. In particular,

$$\frac{1}{s-1} < \zeta(s) < 1 + \frac{1}{s-1}.$$

In particular, the Riemann-Zeta function can also be written in the *Euler product* form, given by

$$\zeta(s) = \prod_{p \text{ prime}} \left(\frac{1}{1-p^{-s}}\right).$$

Taking the log of both sides, we get that

$$\log \zeta(s) = -\sum_p \log(1-p^{-s}).$$

From here on, we simply write a subscript of p on summations or products to indicate that they're prime (unless stated otherwise). Clearly, the above is divergent for $s = 1$.

Lemma 2.3. (i) For all $s_0 > 1$, there exists some constant $M > 0$ such that

$$\log\left|\sum_p p^{-s} - \log\frac{1}{s-1}\right| < M \text{ for all } 1 < s \leq s_0.$$

(ii) The sum of $\frac{1}{p}$ over all primes diverge.

Proof. We may rewrite the equation in the first line as follows,

$$\sum_p p^{-s} = \log\frac{1}{s-1} + O(1) \text{ as } s \to 1,$$

where we may note $O(1)$ is some bounded function. Recall the following,

Definition 2.4. Let f, g be functions on some space X, where $g \geq 0$. We say that $f = O(g)$ if $|f| \leq Mg$, where M is some constant.

In this manner, saying $f = O(1)$ is equivalent to saying that $|f|$ is bounded. Now, let us take the log of the entire following inequality,

$$\begin{gathered}\frac{1}{s-1} < \zeta(s) < 1 + \frac{1}{s-1} = \frac{s}{s-1},\\ \log\left(\frac{1}{s-1}\right) < -\sum_p \log(1-p^{-s}) < \log\left(\frac{s}{s-1}\right), \qquad (*)\\ 0 < -\left(\log(s-1) + \sum_p \log(1-p^{-s})\right) < \log s\end{gathered}$$

where the Taylor expansion of $|-\log(1-p^{-s}) - p^{-s}|$ is less than p^{-2s}.

Exercise 2.5. Check that $|-\log(1-y) - y| < y^2$ for $0 < y < 1$ for $y \in \mathbb{R}$. This is done by expanding $\log(1+x)$ around $x = 0$.

Specifically, summing over all p and applying the triangle inequality, the above tells us that

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

Using both inequalities together, we obtain

$$\begin{aligned}&\left|\sum_p p^{-s} - \log\frac{1}{s-1}\right|\\ &= \left|\left(\sum_p p^{-s} + \sum_p \log(1-p^{-s})\right) - \left(\log\frac{1}{s-1} + \sum_p \log(1-p^{-s})\right)\right|\\ &\leq \zeta(2) + \log s \leq \zeta(2) + s_0 - 1,\end{aligned}$$

if $1 < s \leq s_0$. Indeed, this shows that $M = s_0 - 1 + \zeta(2)$ for (i). The second part of the lemma is also left as homework. $\square$

We now discuss Dirichlet series and Dirichlet L-functions. Let $m \in \mathbb{N}$, and let $(\mathbb{Z}/m\mathbb{Z})^*$ be the invertible elements in the ring $\mathbb{Z}/m\mathbb{Z}$. Specifically, these are the residues modulo m which are prime to m. This forms an abelian group under multiplication, of which its size is given by the totient $\varphi(m)$.

Exercise 2.6. If m is prime, then $(\mathbb{Z}/m\mathbb{Z})^*$ is the cyclic group of order $m-1$.

Fix a character $\chi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$, where $\mathbb{C}^*$ are the nonzero complex numbers. Extend χ as a map $\mathbb{Z} \to \mathbb{C}$ such that $\chi(n)\chi(m) = \chi(nm)$ as follows,

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

As an example, let $m = 3$, and consider $(\mathbb{Z}/3\mathbb{Z})^* = \{\pm 1\}$. Then

$$\chi(n) = \begin{cases} 0 & \text{if } 3 \mid n, \\ 1 & \text{if } n \equiv 1 \pmod 3, \\ -1 & \text{if } n \equiv -1 \pmod 3. \end{cases}$$

For all m, we have the trivial homomorphism $(\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$. Let $\chi : \mathbb{Z} \to \mathbb{C}$ be the function

$$\chi(n) = \begin{cases} 1 & \text{if } \gcd(n,m) = 1, \\ 0 & \text{if } \gcd(n,m) \neq 1. \end{cases}$$

Then we may define the L-function

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(\frac{1}{1 - \frac{\chi(p)}{p^s}} \right).$$

Claim 2.7. $L(\chi, x)$ is absolutely convergent for $\Re s > 1$.

Theorem 2.8. (i) $L(\chi, s)$ is holomorphic for $\Re s > 1$. (ii) Assume the extension of χ is not equal to 1. Then $L(\chi, s)$ converges for $\Re s > 0$ and defines a holomorphic function there. (iii) If the extension of χ is not equal to 1, then $L(\chi, 1) \neq 0$.

Let G be a finite abelian group. Consider all characters $\chi : G \to \mathbb{C}^*$; they form a group $G^\vee$ under multiplication.

Claim 2.9. (i) $G^\vee$ is (non-canonically) isomorphic to G, and $\#G^\vee = \#G$. (ii) $(G^\vee)^\vee \cong G$ canonically.

Proof. The claim lets us say that if G is finite and abelian, then G is isomorphic to a product of finite cyclic groups

$$G \cong \prod_{i=1}^{k} (\mathbb{Z}/a_i\mathbb{Z}), \qquad a_i > 1.$$

Using the fact that $(G \times H)^\vee \cong G^\vee \times H^\vee$, we see that specifying $\chi : G \times H \to \mathbb{C}^\times$ is equivalent to specifying characters χ_1, χ_2 on G and H respectively. Letting $a > 1$, we have that if $\chi : \mathbb{Z}/a\mathbb{Z} \to \mathbb{C}^\times$ and $g^a = 1$, we have that $\chi(g) \in \mathbb{C}^*$ and $\chi(g)^a = 1$. This means that $\chi(g)$ must be an ath root of unity. All the roots of 1 of order a form a cyclic group of order a.

For the second part of the claim, in the direction of $G \to (G^\vee)^\vee$, we have that for each $g \in G$, we obtain a canonical map $G^\vee \to \mathbb{C}^*$ where all $x \in G^\vee \mapsto \chi(g)$. $\square$

Lemma 2.10. This map is an isomorphism.

Lemma 2.11. (i) All $\chi \in G^\vee$ form a basis of $\mathbb{C}(G)$, the complex valued functions on G. (ii) This basis is orthonormal with respect to $\langle f_1, f_2 \rangle = \frac{1}{\#G} \sum_g f_1(g)\bar{f}_2(g)$.

Proof. We know that $\dim \mathbb{C}(G) = \#G = \#G^\vee$. Recall that we have

$$\langle \chi, \chi \rangle = \frac{1}{\#G} \sum_g \chi(g)\bar{\chi}(g) = \frac{1}{\#G} \sum_g \chi(g)\chi_g^{-1} = \frac{1}{\#G} \sum_g \chi(gg^{-1}) = 1,$$

since $\chi(1) = 1$. Now, let us evaluate $\#G \langle \chi, 1 \rangle = \sum_g \chi(g)$. We have that since χ is not uniformly 1, there must exist some $h \in G$ such that $\chi(h) \neq 1$; and so

$$\chi(h) \sum_g \chi(g) = \sum_g \chi(hg) = \sum_g \chi(g),$$

meaning $\sum_g \chi(g) = 0$, as $\chi(h)$ is nonzero as well. Thus, we obtain that

$$\#g \langle chi_1, \chi_2 \rangle = \sum_g \chi_1(g)\bar{\chi_2}(g) = \sum_g \chi_1(g)\chi_2^{-1}(g),$$

meaning that $\#G = \left\langle \chi_1\chi_2^{-1}, 1 \right\rangle$. If $\chi_1\chi_2^{-1} \neq 1$ (i.e., if $\chi_1 \neq \chi_2$), then this is 0. $\square$

Let x_n be a sequence of elements of $\mathbb{R}_{>0}$ such that $\lim_{n\to\infty} \lambda_n = \infty$. The main example we will be looking at is $\lambda_n = \log n$ (or $\lambda_n = n$), and the Dirichlet series $\sum_n a_n e^{-\lambda_n z}$ where $a_n \in \mathbb{C}$.

Next lecture, we will do some general analysis of convergence and analytic properties of such series. We will apply this to $L(\chi, s)$.

§3 Day 3: Characters (Sep. 9, 2025)

Recall that given $m \in \mathbb{Z}_{\geq n}$, we have $\chi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ and $\tilde{\chi} : \mathbb{Z} \to \mathbb{C}$ satisfies

$$\tilde{\chi}(n) = \begin{cases} 0 & n \text{ is not prime to } m, \\ \chi(n, \operatorname{mod} m) & \text{if } \gcd(n, m) = 1. \end{cases}$$

Also, we ask that $|\chi(n)| \leq 1$ for all n (so the magnetude does not spiral off to infinity). Recall that the L-function is defined as

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

which converges absolutely for $\Re s > 1$. Then we have the following theorem,

Theorem 3.1. $L(\chi, s)$ is holomorphic in s for $\Re s \geq 1$, and it extends meromorphically to $\Re s > 0$. If $\chi \neq 1$, then $L(\chi, s)$ is holomorphic for $\Re s > 0$ and the series $\sum \frac{\chi(n)}{n^s}$ is convergent for $\Re s > 0$. Moreover, if $\chi = 1$, then $L(\chi, s)$ has a simple pole at $s = 1$ and has no other poles.

In fact, $L(\chi, s)$ is meromorphic for all $s \in \mathbb{C}$.

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

We plan to prove theorem 3.1, then, assuming theorem 3.2, we will deduce the Dirichlet theorem about primes in an arithmetic progression. We will follow Serre's book here (section 2.2, Dirichlet series).

Let x_n be a seqeucne of positive real numbers tending to infinity, i.e., $\lim_{n\to\infty} \lambda_n = \infty$. A *Dirichlet series* is a series, where, given $\{a_n\}$ a sequence of complex numbers, we write

$$\sum_{n=1}^{\infty} a_n e^{-\lambda_n z}, \qquad (a_n \in \mathbb{C}, z \in \mathbb{C}).$$

Two such examples of Dirichlet series are given by setting $\lambda_n = \log n$ (the ordinary Dirichlet series), where such a series is written $\sum \frac{a_n}{n^s}$, and $\lambda_n = n$ where by setting $t = e^{-z}$, the series turns into a power series in t as follows,

$$\sum_{n=1}^{\infty} a_n e^{-nz} = \sum_{n=0}^{\infty} a_n t^a.$$

Theorem 3.3. Assume that $f(z) = \sum_{n=0}^{\infty} a_n e^{-\lambda_n z}$ is convergent for $z = z_0$. Then it is convergent uniformly on every set of the form $\Re(z - z_0) \geq 0$, where $\arg(z - z_0) \leq \alpha$ with $\alpha < \frac{\pi}{2}$.

Exercise 3.4. Analyze what this means for $\lambda_n = n$ and realize that you know this statement.

Lemma 3.5. Suppose $\{f_n(z)\}$ is a sequence of holomorphic functions on some domain $U \subset \mathbb{C}$. Assume there exists $f(z) = \lim_{n\to\infty} f_n(z)$ for all $z \in U$ such that the convergence is uniform on every compact subset of U. Then $f(z)$ is holomorphic, and moreover, $f'(z) = \lim_{n\to\infty} f_n'(z)$.

In particular, if we let $U = \{z \mid \Re(z) > \Re(z_0)\}$, then every compact set can be covered by finitely many sectors, meaning there exists a uniform convergence no every compact set.

Corollary 3.6. Let $L(\chi, s)$ be holomorphic for $\Re s > 1$.

The following lemma is necessary to study series with summands of the form $a_n b_n$.

Lemma 3.7 (Abel's lemma)**.** Let $A_{m,p} = \sum_{n=m}^{p} a_n$ and let $B_{m,m'} = \sum_{n=m}^{m'} a_n b_n$. Then we have

$$S_{m,m'} = \sum_{n=m}^{m'-1} A_{m,n}(b_n - b_{n+1}) + A_{m,m'} b'_m.$$

Lemma 3.8. Let $\alpha, \beta \in \mathbb{R}$, and let $0 < \alpha < \beta$. Then $z = x + iy$ with $x > 0$; then

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

For $z = z_0$, $f(z_0)$ converges and $\sum a_n$ convegres, meaning that for all ε, there exists N such that for all $m, m' \geq N$, we have that $\left| A_{m,m'} \right| < \varepsilon$. Applying the lemma with $b_n = e^{-\lambda_n z}$, we have that

$$S_{m,m'} = \sum_{n=m}^{m'-1} A_{m,n}(e^{-\lambda_n z} - e^{-\lambda_{n+1} z}) + A_{m,m'} e^{-\lambda_{m'} z},$$

and putting $z = x + iy$ and applying lemma 3.8, we have that

$$\left| S_{m,m'} \right| \leq \varepsilon \left(1 + \frac{|z|}{x} \sum_{n=m}^{m'-1} \left(e^{-\lambda_n x} - e^{-\lambda_{n+1} x} \right) \right) \leq \varepsilon (1 + k(e^{-\lambda_m x} - e^{\lambda_{m'} x})) \leq e(1 + k),$$

and so uniform convergence is clear. Note that I am not entirely confident about this argument, so re-check the proof of proposition 6 in Serre's book if confused.