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. □

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. □

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.,

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

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

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

and

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

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

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

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

(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 $g \ge 0$. We say that $f = O(g)$ if $|f| \le Mg$, 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,

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

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

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

if $1 < s \le s_0$. 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 $x \in G^\vee \mapsto \chi(g)$. ☐

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.

§4 Day 4: (Sep. 11, 2025)

Last time, we proved that $L(\chi, s)$ are holomorphic for $\Re s > 1$, up to some lemma; next, we are going to show that all $L(s, \chi)$ are in fact, meromorphic, for $\Re s > 0$.

1. (Page 71, Prop. 11) If $\chi = 1$, then $\zeta(s)$ is meromorphic for $\Re s > 0$ and has a unique simple pole for $s = 1$.

2. (Prop. 12) If $\chi \neq 1$, then $L(s, \chi)$ is holomorphic for $\Re s > 0$.

Later today, we will show that (prop. 13)

$$\zeta_m(s) = \prod_{\chi} L(s, \chi) \iff \forall x, x \neq 1, L(1, \chi) \neq 0.$$

We note that ζ_m has a simple pole at $s = 1$. W ealso have the unproved lemma from last time, where if $0 < \alpha < \beta$, then for $z \in \mathbb{C}$ with $\Re z > 0$, written $z = x + iy$, we have that

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

This is true by writing

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

We now discuss proposition 10. In the case $\chi = 1$, we claim the following,

Claim 4.1 (Prop. 10)**.** $\zeta(s) = \frac{1}{s-1} + \varphi(s)$, where $\varphi(s)$ is holomorphic in $\Re s > 0$.

Proof. We have that

$$\frac{1}{s-1} = \int_1^{\infty} t^{-s} \, dt = \sum_{n=1}^{\infty} \int_n^{n+1} t^{-s} \, dt,$$

meaning we may write

$$\zeta(s) = \frac{1}{s-1} + \sum_{n=1}^{\infty} \int_n^{n+1} \left(n^{-s} - t^{-s} \right) \, dt.$$

With this, we may construct a sequence of φ_n,

$$\varphi_n(s) = \int_n^{n+1} \left(n^{-s} - t^{-s} \right) \, dt, \quad \varphi(s) = \sum_{n=1}^{\infty} \varphi_n(s),$$

where each $\varphi_n(s)$ is holomorphic for $\Re s > 0$. Since each $\varphi_n(s)$ holds this property, it suffices to check that the series converges normally, of which we have that $\sum_{n=1}^{\infty} \|\varphi_n\|$ converges, where $\|\varphi_n\| = \sup_{s \in S} |\varphi_n(s)|$. We claim that normal convergence implies uniform absolute convergence, i.e., for all $\varepsilon > 0$, the series of $\varphi_n(s)$ is normally convergent in $\Re s \geq \varepsilon$.

Subproof. To start, let us make the naive bound

$$\|\varphi_n(s)\| \leq \sup_{n\leq t\leq n+1} \left|n^{-s} - t^{-s}\right| \leq \sup_{n\leq t\leq n+1} \left|\frac{dt^{-s}}{dt}\right|,$$

which we have from the lemma that if f is a continuously differentiable function, we have that

$$|f(a) - f(b)| \leq \sup_{a\leq x\leq b} \left|f'(x)\right|(b-a).$$

In this manner, we also have that

$$\sup_{n\leq t\leq n+1} \left|\frac{dt^{-s}}{dt}\right| = \sup_{n\leq t\leq n+1} \left|\frac{s}{t^{s+1}}\right| = \frac{|s|}{n^{x+1}},$$

where we have that on $\Re s \geq \varepsilon$, $\sum_n \frac{|s|}{n^{s+1}}$ is convergent. ■

Claim 4.2. $L(s,\chi)$ converges for $\Re s > 0$.

By what we did last time, this implies that $L(s,\chi)$ is holomorphic in $\Re s > 0$. □

Conjecture 4.3 (Riemann Hypothesis)**.** For $\Re s > 0$, the only zeros of $\zeta(s)$ have $\Re = \frac{1}{2}$.

We will discuss the motivations and applications for this later. We start by considering the section post-proposition 12,

Lemma 4.4 (Proposition 9)**.** Suppose we have a series $\sum a_n n^{-s}$. Assume that all partial sums of $\{a_n\}$ are bounded; if all $A_{m,m'}$, given by

$$A_{k,k'} = \sum_{n=k}^{k'} a_n,$$

are bounded, then $\sum a_n n^{-s}$ is convergent for $\Re s > 0$.

Consider the function,

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

if we let $a_n = \tilde{\chi_n}$, then for all k, we have that

$$\sum_{n=k}^{k+m-1} \tilde{\chi}(n) = 0.$$

Proof. Assume all $\left|A_{k,k'}\right| \leq K$; by applying Abel's lemma, we have that

$$\left|S_{k,k'}\right| = \left|\sum_{n=k}^{k'} a_n \underbrace{n^{-s}}_{b_n}\right| \leq K\left(\sum_{n=k}^{k'}\left|\frac{1}{n^s} - \frac{1}{(n+1)^s}\right| + \left|\frac{1}{(k')^s}\right|\right).$$

If $\Re s > 0$, then the right hand side is simply equal to $\frac{K}{k^s}$, andfor all $\varepsilon > 0$, there exists N such that if $k \geq N$, then the $\frac{K}{k^s} \leq \varepsilon$. □

So far, we've proven that

(i) For all χ, $L(s,\chi)$ is meromorphic for $\Re s > 0$.

(ii) If $x = 1$, there is a unique simple pole at $s = 1$.

(iii) If $x \neq 1$, there are no poles.

Finally, we need that $L(1, \chi) \neq 0$ if $\chi \neq 1$ (p.73, thm. 1). Define

$$\zeta_m(s) = \prod_x L(s, \chi),$$

which we already know to be meromorphic for $\Re s > 0$. We want to show that $\zeta_m(s)$ has a unique simple pole at $s = 1$. As a quick digression, consider $\mathbb{Q} \subset K \subset \mathbb{C}$, where K is a finite extension of $\mathbb{Q}$ (equivalently, $\dim_{\mathbb{Q}}(K) < \infty$). There exists a notion that $\zeta_K(s)$, which is a ζ function of a number field K. All of those have analytic properties similar to $\zeta(s)$. We have that $\zeta(s) = \zeta_{\mathbb{Q}}(s)$ has a unique simple pole at $s = 1$; if we fix $m \geq 1$, then the cyclotomic field of order m, K_m, is given by $K_m = \mathbb{Q}(\mu_m) = K(e^{2\pi \frac{t}{m}})$, where μ_m are the roots of 1 of order m. Secretly, we have that $\zeta_m(s) = \zeta_{K_m}(s)$.

We write out the explicit Dirichlet series for $\zeta_m(s)$. Let p be a prime that does not divide into m, i.e., $\overline{p} = (\mathbb{Z}/m\mathbb{Z})^* = G(m)$. Let $f(p)$ be the order of $\overline{p}$ in $G(m)$, and let $g(p) = \frac{f(m)}{f(p)}$, which is the order of $G(m)$ quotiented by the subgroup generated by $\overline{p}$.

Claim 4.5 (Proposition 13)**.** We have that

$$\zeta_m(s) = \prod_{p \nmid m} \left(\frac{1}{1 - p^{-f(p)s}} \right)^{g(p)}.$$

Proof. Let T be a variable. Fix p where $p \nmid m$; then we have

$$\prod_{\chi} (1 - \chi(\overline{p})T) = (1 - T^{f(p)})^{g(p)},$$

which follows from

$$\prod_w (1 - wT) = 1 - T^{f(p)},$$

and the product is taken over all w where $w^{f(p)} = 1$, i.e., the $f(p)$-th roots of unity (we note that $f(p)$ can be any element of $\mathbb{N}$). For all such w, there exist $g(p)$ characters χ such that $\chi(\overline{p}) = w$, which implies our result. To see why this is true, let A be a finite abelian group, $B \subset A$ a subgroup, and let $\chi_B : B \to \mathbb{C}^*$. Then there exists exactly $\#(A/B)$ extensions of χ_B to A.

In our case, let $A = (\mathbb{Z}/m\mathbb{Z})^*$, B be the subgroup generated by $\overline{p}$, and fix w such that $w^{f(p)} = 1$. There exists a unique character χ_B of B such that $\chi_B(\overline{p}) = w$. An extension to A is a character $\chi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ such that $\chi(\overline{p}) = w$, and so

$$g(p) = \# \frac{(\mathbb{Z}/m\mathbb{Z})^*}{B},$$

meaning that for all w with $w^{f(p)} = 1$, there exist $g(p)$ characters χ such that $\chi(\overline{p}) = w$. Consider the chain

$$0 \to B \to A \to A/B \to 0.$$

If we let $\widehat{\cdot}$ denote the dual groups,

$$0 \to \widehat{A/B} \xrightarrow{\alpha} \widehat{A} \xrightarrow{\beta} \widehat{B} \to 0,$$

then we claim that $\widehat{A/B} \to \widehat{A}$ is injective, and $\ker \beta = \operatorname{im} \alpha$, which is obvious; since $\#A = \#\widehat{A}$, we have that $\widehat{A} \xrightarrow{\beta} \widehat{B}$ is onto, and we are done. $\square$

§5 Day 5: Density (Sep. 16, 2025)

Recall that last time, we discussed that given $m > 0$, we have that

$$\zeta_m(s) = \prod L(\chi, s) = \prod_{p \nmid m} \left(1 - p^{-f(p)}\right)^{-g(p)},$$

where the first product is taken over all characters of $(\mathbb{Z}/m\mathbb{Z})^*$. We have that $f(p)$ denotes the order of $\overline{p}$, the imag eof p, in $(\mathbb{Z}/m\mathbb{Z})^*$, and $g(n)$ the number of quotients of $(\mathbb{Z}/m\mathbb{Z})$ by the span generated by $\overline{p}$.

Theorem 5.1. $\zeta_m(s)$ has a pole of order 1 at $s = 1$.

Corollary 5.2. $L(\chi, 1) \neq 0$ for all nontrivial characters.

Today, we will use this for the Dirichlet theorem; we will give a more precise formulation of the Dirichlet theorem, and define the notion of density of some set $A \subset \underline{P}$, where $\underline{P}$ is the set of all primes.

Lemma 5.3 (4.1)**.** Given $s \in \mathbb{R}_{>1}$, we have that $\sum_p p^{-s} \sim -\log(s-1)$ as $s \to 1$, i.e., the ratio approaches 1 as $s \to 1$.

Specifically, we have

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

Using the fact that $\zeta(s)$ has a pole of order 1 at $s = 1$, we have that, for $s \in \mathbb{R}_{>1}$,

$$\log \zeta(s) = \sum_{p \in \underline{P}} -\log(1 - p^{-s}) = \sum_{p,k=2}^{\infty} \frac{1}{kp^{ks}} - \frac{1}{p^{ks}} \leq \frac{1}{p^s(p^s - 1)}.$$

It is sufficient to show that $\sum \frac{1}{kp^{ks}}$ remains bounded when $s > 1$, which we readily see from

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

If $A \subset \underline{P}$, we say that A has *density* $k \in \mathbb{R}$ if

$$\lim_{\substack{s \to 1 \\ s > 1}} \frac{\left(\sum_{p \in A} \frac{1}{p^s}\right)}{-\log(s-1)} = k;$$

clearly, $0 \leq k \leq 1$. We remark that if $k > 0$, then A is an infinite set (all finite A has density zero).

Remark 5.4. Let $P \subset \mathbb{N}$ be any infinite subset, and let $A \subset \underline{P}$. The natural density is defined as

$$\lim_{n \to \infty} \frac{\#\{i \in A \mid i \leq n\}}{\#\{i \in \underline{P} \mid i \leq n\}},$$

of which we note this is a stronger notion, since if $A \subset \underline{P}$ has natural density k, then it has density k, but the opposite direction is not necessarily true.

Theorem 5.5. Let $m > 0$, $\gcd(a, m) = 1$. The set $\underline{P}_a$ of all primes which are congruent to $a \bmod m$ has density $\frac{1}{\varphi(m)}$.

We note that the above is also true for natural density. To prove the theorem, we'll need to know that $L(\chi, 1) \neq 0$ for $\chi \neq 1$. Assuming this is true, we will give the proof as follows; define f_χ,

$$f_\chi(s) = \sum_{p \nmid m} \frac{\chi(p)}{p^s},$$

where $s \in \mathbb{R}_{>1}$ for $s \in \mathbb{C}$ with real part greater than 1. To start, observe that $f(1) \sim -\log(s-1)$ as $s \to 1$; this differs from $\sum_{p \in \underline{P}} p^{-s}$ by finitely many terms. For $\chi \neq 1$, we have that f_χ is bounded where $s > 1$; let $g_a(s) = \sum_{p \in P_a} p^{-s}$, and let us claim that

$$g_a(s) = \frac{1}{\varphi(m)} \sum_\chi \chi(a)^{-1} f_\chi(s).$$

This yields that $f_\chi(s) \sim -\log(s-1)$, where, if $\chi = 1$ and bounded if $\chi \neq 1$, then we have that

$$\lim_{s \to 1} \frac{f_\chi(s)}{-\log(s-1)} = \begin{cases} 0 & \chi \neq 1, \\ 1 & \chi = 1. \end{cases} \implies \lim_{s \to 1} \frac{g_a(s)}{-\log(s-1)} = \frac{1}{\varphi(m)}.$$

To fill in the gaps in the above proof outline, observe that

$$\sum_\chi \chi(a)^{-1} f_\chi = \sum_{\chi, p \nmid m} \frac{\chi(a)^{-1}\chi(p)}{p^s}, \quad \sum_\chi \chi(a^{-1}p) = \begin{cases} \varphi(m) & \text{if } a^{-1}p \equiv 1 \bmod m, \\ 0 & \text{otherwise.} \end{cases}$$

More generally, for G-finite abelian groups, we have that

$$\sum_{x \in \widehat{G}} \chi(g) = \begin{cases} \#G & g = 1, \\ 0 & g \neq 1. \end{cases}$$

Moreover, $f_\chi(s) = \sum_{p \nmid m} \frac{\chi(p)}{p^s}$ remains bounded as $s \to 1$, and for $\log L(\chi, s)$, we have that

$$\log \prod_{p \nmid m} \left(1 - \chi(p)p^{-s}\right)^{-1} = \sum_{p \nmid m} \sum_{k=1}^{\infty} \frac{\chi(p)^k}{kp^{ks}} = f_\chi(s) \underbrace{\sum_{p, k \geq 2} \frac{\chi(p)^k}{kp^{ks}}}_{=:B(s)}.$$

In this way,

$$|B(s)| = \sum_{p, k \geq 2} \frac{1}{kp^{ks}},$$

which is bounded above as $s \to 1$, so $B(s)$ itself is bounded.

§6 Day 6: Quadratic Reciprocity (Sep. 18, 2025)

Our plan for today is to finish the proof that $L(\chi, 1) \neq 0$ for all $\chi \neq 1$, and find an example of explicit number theoretic applications. This example will require the law of quadratic reciprocity, which we wlil discuss (in chapter 1 of Serre's book).

Let $\zeta_m(s) = \prod L(\chi, s)$, taken over the characters of $(\mathbb{Z}/m\mathbb{Z})^*$. We want to show that ζ_m has a pole at $s = 1$.

$$\zeta_m(s) = \prod_{p \nmid m} \left(1 - \frac{1}{p^{-f(p)s}}\right)^{-g(p)},$$

where $f(p)$ is the order of $\overline{p}$, i.e., the image of p in $(\mathbb{Z}/m\mathbb{Z})^*$, and $g(p) = \frac{\#\varphi(m)}{f(p)}$. With this, we see that $\zeta_m(s)$ further equals

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

If we expand $\prod_{p \nmid m}$, we get $\sum a_n n^{-s}$, where $a_n \geq 0$.

Lemma 6.1. Let $f = \sum a_n e^{-\lambda_n z}$ be a Dirichlet series such that $a_n \in \mathbb{R}_{\geq 0}$ and $\{\lambda_n\}$ is an increasing sequence of real numbers with $\lambda_n \to +\infty$, there exists $\rho \in \mathbb{R}$ such that $f(z)$ is convergent for $\Re z > \rho$, and assume that f analytically continues to a neighborhood of ρ. Then there exists $\varepsilon > 0$ such that $f(z)$ is convergent for $\Re z > \rho - \varepsilon$.

A similar statement states that if $f(z) = \sum_{n=0}^{\infty} a_n (z - \alpha)^n$ converges absolutely for $|z - \alpha| < r$ and extends analytically to $|z - \alpha| < R$, then $\sum a_n (z - \alpha)^n$ converges absolutely for $|z - \alpha| < R$.

We will not prove our lemma here; said lemma implies that if $\zeta_m(s)$ has no pole at $s = 1$, then its Dirichlet series is convergent for $\Re s > 0$. If

$$\zeta_m(s) = \prod_{p \nmid m} \left(1 + p^{-f(p)s} + p^{-2f(p)s} + \dots\right)$$

is convergent for $s \in \mathbb{R}$, then

$$\prod_{p \nmid m} \left(1 + p^{-\varphi(m)s} + p^{-2\varphi(m)s} + \dots\right)$$

is convergent, meaning that the above is equal to $\sum_{n=1}^{\infty} n^{-\varphi(m)s}$, which we know is divergent for $s = \frac{1}{\varphi(m)}$, yielding a contradiction. This concludes our work with this section of Serre's textbook.

We now move onto quadratic reciprocity (chapter 1 in Serre).

Claim 6.2. Let $a \in \mathbb{Z}$. If the equation $x^2 = a$ has a solution mod p (i.e., in $\mathbb{Z}/p\mathbb{Z}$) for almost all p (all but finitely many), then m is a square ($x^2 = a$ has a solution in $\mathbb{Z}$).

Definition 6.3 (Legendre Symbol)**.** Let p be prime, $a \in \mathbb{Z}$, and write

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } p \nmid a \text{ and } a \text{ is a square mod } p, \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is not a square mod } p. \end{cases}$$

In particular, for fixed p, we have that $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Proposition 6.4. Let $a \neq 0$ be a squarefree integer. Let $m = 4\,|a|$. Then there exists a unique character χ_a of $(\mathbb{Z}/m\mathbb{Z})^*$ such that $\chi_a(p) = (\frac{a}{p})$ for all $p \nmid m$. We have that $\chi_a^2 = 1$.

This proposition requires quadratic reciprocity.

Corollary 6.5. Let $a \in \mathbb{Z}$ not be a square. Then the set of all p such that $(\frac{a}{p}) = 1$ has density $\frac{1}{2}$ (Dirichlet density).

The corollary follows from the proposition and the Dirichlet theorem. We can assume that a is square by taking $m = 4\,|a|$. Let $H \subset (\mathbb{Z}/m\mathbb{Z})^*$ be the kernel of χ_a, and let $p \nmid m$; let $\overline{p} \in (\mathbb{Z}/m\mathbb{Z})^*$. Then $\chi_a(p) = 1$ if and only if $p \in H$. We have that

$$|H| = \frac{\varphi(m)}{2} = \frac{\#(\mathbb{Z}/m\mathbb{Z})^*}{2}.$$

For all $x \in (\mathbb{Z}/m\mathbb{Z})^*$, the density of primes p such that $\overline{p} = x$ is $\frac{1}{\varphi(m)}$, which implies that the density of p such that $\overline{p} \in H$ is exactly $\frac{1}{2}$. In the claim, the density of p such that $(\frac{a}{p}) = 1$ is assumed to be 1, we have that a has to be a square.

Quadratic reciprocity compares $(\frac{p}{q})$ with $(\frac{q}{p})$ where p, q are primes. Let n be an odd integer. Then define $\varepsilon(n) = \pm 1$, given by $\frac{n-1}{2} \bmod 2$.

Theorem 6.6 (Quadratic Reciprocity)**.** Using ε as defined above, we have that

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

The law of quadratic reciprocity is a special case of a much more general series of reciprocity laws in class field theory (this is a baby case of Langlands identity).

Let p be a prime, and consider $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (this is a field).

Lemma 6.7. $\mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group of order $p - 1$.

Corollary 6.8. If $p \nmid a$ and $p \neq 2$, then $(\frac{a}{p}) = a^{\frac{p-1}{2}} \bmod p$.

We see this from $a^{p-1} \equiv 1 \bmod p$, so $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$, which is given by the Legendre symbol $(\frac{a}{p})$. If we write $\overline{a} = \overline{b}^2$, then $\overline{a}^{\frac{p-1}{2}} = \overline{b}^{p-1} = 1$ in $\mathbb{F}_p^*$.

Exercise 6.9. If we know that $\mathbb{F}_p^*$ is cyclic, then the converse of this is true.

Lemma 6.10. Let G be a cyclic group of order $2n$. $g \in G$ is a square if and only if $g^n = 1$.

Let K be any field. Then either $n \cdot 1_K \neq 0$ for all nonzero integers n (and in this case $K \supset \mathbb{Q}$ and is said to have characteristic $\mathbb{Q}$), or p is prime and $\{n \in \mathbb{Z} \mid n \cdot 1_K = 0\} = \{pk \mid k \in \mathbb{Z}\}$. Here, p is called the characteristic of K, and in this case, $K \supset \mathbb{F}_p$, which is the finite field with p elements. If K is finite, then $\operatorname{char} K = p > 0$, and $\mathbb{Z} \to K$ given by $n \mapsto n \cdot 1_K$ cannot be injective. We have that $K \supset \mathbb{F}_p$ for some p, and K is a finite dimensional vector space over $\mathbb{F}_p$. This means $K \cong \mathbb{F}_p^n \implies \#K = p^n = q$.

For all p, n, there exists a unique (up to isomorphism) field $\mathbb{F}_q$ such that $\#\mathbb{F}_q = q = p^n$. Let K be the algebraic closure of $\mathbb{F}_p$ (unique up to isomorphism). If K is any field of characteristic p, then $x \mapsto x^p$ is an automorphism of K, which we may readily check

$$(xy)^p = x^p y^p, \quad (x + y)^p = x^p + y^p,$$

and the same is true for $x \mapsto x^q = x^{p^n}$. Let $\{x \in K \mid x^q = x\}$ be a subfield. Its size is the number of roots of $x^q - x$; we see that $(x^q - x)' = qx^{q-1} - 1 = -1$, where $x^q - x \in K[x]$. Since $\gcd(x^q - x, (x^q - x)') = 1$, we see that there are no multiple roots, and so said subfield is given by $\mathbb{F}_q$ and has q elements.

If L has q elements, then for all $x \in L$, $x^q = x$, i.e., for $x \neq 0$, we have $x^{q-1} = 1$, and $L^* = L \setminus \{0\}$ is a group under multiplication, where $\#L^* = q - 1$, and $x^{q-1} = 1$ for all $x \in L^*$.

Lemma 6.11. For all $q = p^n$, the group $\mathbb{F}_q^*$ is cyclic of order $q - 1$.

Lemma 6.12. For $n \geq 1$, $n = \sum_{d|n} \varphi(d)$.

Lemma 6.13. Let H be a finite group of order n. Assume that, for all $d \mid n$, $\#\{x \in H \mid x^d = 1\} \leq d$. Then H is cyclic of order n.

We prove the last two lemmas, since the first follows from our earlier discussion. We start with lemma 6.13.

Proof. If there exists $x \in H$ of order d, then $\#\{1, x, x^2, \ldots, x^{d-1}\} = d$. This means for all $g \in H$, $g^d = 1$, then $y = x^i$, where $i \in [d]$. This means $\#\{x \in H \mid \operatorname{ord} x = d\} = \varphi(d)$. Lemma 6.12 implies that $\{x \mid \operatorname{ord} x = d\}$ is nonempty, and so

$$\#H = n = \sum_{d|n} \#\{x \in H \mid \operatorname{ord} x = d\},$$

and we know that it is given by either $\varphi(d) = 0$. Lemma 6.12 states that it is $\varphi(d)$ for all d. In this way, we can take $n = d$ to see that $\{x \in H \mid \operatorname{ord} x = n\}$ is nonempty, and we conclude. $\square$

Take $H = \mathbb{F}_q^*$, where $q = p^n$. We have that $\#\mathbb{F}_q^* = p^n = 1$, and let d be a divisor of $q - 1$. Then $\{x \mid x^d = 1\} \leq d$, i.e., the set of roots of $x^d - 1$, which has at most d roots.

Lemma 6.14. (i) $(\frac{1}{p}) = 1$, (ii) $(\frac{-1}{p}) = (-1)^{\varepsilon(p)}$, (iii) $(\frac{2}{p}) = (-1)^{\omega(p)}$, where $\omega(n) = \frac{n^2-1}{8} \bmod 2$ for odd integers n.

Let K be the algebraic closure of $\mathbb{F}_p$. Let α be the primitive 8th root of 1, where $\alpha^8 = 1$, $\alpha^i \neq 1$ for $1 \leq i \leq 8$. We have that $y = \alpha + \alpha^{-1}$ and $y^p = \alpha^p + \alpha^{-p}$ in general, where $\alpha^4 = -1$, $\alpha^2 + \alpha^{-2} = 0$, so $y^2 = \alpha^2 + \alpha^{-2} + 2 = 2$. This means that if p satisfies $y^p = -y$, we have $y \notin \mathbb{F}_p$. This means if $p \equiv \pm 1 \bmod 8$, then $y^p = y$ implies $y \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$; specifically, $y^2 = 2$ means 2 is a square modulo p, and if $p \equiv \pm 5 \bmod 8$, we have a similar argument to follow.

§7 Day 7: Law of Quadratic Reciprocity (Sep. 23, 2025)

Today, our main objective is to prove the law of quadratic reciprocity, and discuss an application from last lecture. Let p, ℓ be distinct odd primes; then recall that we have

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

where $\varepsilon(p) = \frac{p-1}{2} \bmod 2$, which is given by 0 if $p \equiv 1$ modulo 4, and 1 if $p \equiv 3$ modulo 4. In this manner, we have that

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

which was discussed last time. The trick is to use a Gauss sum in a K-algebraically closed field (later, we'll assume that $\operatorname{char} K = p > 0$). Let w be a primitive ℓ-th root of 1¿ As an example, if we take $K = \mathbb{C}$, we may take $w = e^{2\pi i/\ell}$, and the Gauss sum

$$\sum_{x \in \mathbb{F}} \left(\frac{x}{\ell}\right) w^x = y \in K$$

makes sense.

Lemma 7.1. $y^2 = (-1)^{\varepsilon(\ell)}\ell$.

Lemma 7.2. $y^{p-1} = (\frac{p}{\ell})$ if $\operatorname{char} K = p$.

Taking both lemmas together, we have the theorem of quadratic reciprocity, where in particular, in $\mathbb{F}_p$, we have that $(\frac{n}{p}) = n^{\frac{p-1}{2}}$. For all K, we have a map $\mathbb{Z} \to K$ where $n \mapsto n \cdot 1_K$, and so

$$\left(\frac{(-1)^{\varepsilon(\ell)}\ell}{p}\right) = y^{p-1} = \left(\frac{p}{\ell}\right),$$

where the first lemma yields the first equality, and the second lemma the second. We start by proving lemma 2.

Proof. We want $y^p = (\frac{p}{2})y$, for which we need to know the $y \neq 0$ case which will follow from lemma 1. We may write,

$$y^p = \sum_{x \in \mathbb{F}_\ell} \left(\frac{x}{\ell}\right) w^{xp} = \sum_{x \in \mathbb{F}_\ell} \left(\frac{p^{-1}z}{\ell}\right) w^z = \left(\frac{p^{-1}}{\ell}\right) y,$$

since

$$\left(\frac{p^{-1}z}{\ell}\right) = \left(\frac{p^{-1}}{\ell}\right)\left(\frac{z}{\ell}\right), \quad \sum_{x \in \mathbb{F}_\ell} \left(\frac{p^{-1}z}{\ell}\right) w^z = \left(\frac{p^{-1}}{z}\right) \sum_{z \in \mathbb{F}_\ell} w^z.$$

$\square$

In particular, the lemma says that

$$\left(\sum_{x \in \mathbb{F}_\ell} \left(\frac{x}{\ell}\right) e^{2\pi i x/\ell}\right)^2 = (-1)^{\varepsilon(\ell)}\ell.$$

We now work through lemma 1.

Proof. Let $y = \sum_{x\in\mathbb{F}_\ell} (\frac{x}{\ell}) w^x$, and consider that

$$\sum_{x,z\in\mathbb{F}_\ell} \left(\frac{xz}{\ell}\right) w^{x+z} = \sum_{u\in\mathbb{F}_\ell} w^u \left(\sum_{t\in\mathbb{F}_\ell} \left(\frac{t(u-t)}{\ell}\right)\right),$$

for which we note $t(u-t) = tu - t^2$, so

$$\left(\frac{t(u-t)}{\ell}\right) = \left(\frac{-t^2}{\ell}\right)\left(\frac{1-ut^{-1}}{\ell}\right) = (-1)^{\varepsilon(\ell)}\left(\frac{1-ut^{-1}}{\ell}\right),$$

and

$$(-1)^{\varepsilon(\ell)} y^2 = \sum_{u\in\mathbb{F}_\ell} C_u w^u,$$

where $C_u = \sum_{t\in\mathbb{F}_\ell^*} \left(\frac{1-ut^{-1}}{\ell}\right)$, for which we may note that for $u = 0$, we have $C_u = \ell$, and for nonzero u, we have $s = 1 - ut^{-1}$, and so the sums over $\mathbb{F}_\ell \setminus \{1\}$ are given by

$$C_u = \sum_{s\in\mathbb{F}_\ell} \left(\frac{s}{\ell}\right) - \left(\frac{1}{\ell}\right) = -1.$$

In this manner, we may continue our computation from earlier and obtain

$$\sum C_u w^u = (\ell - 1) - \sum_{u\in\mathbb{F}_\ell^*} w^u = \ell,$$

where the latter summation is equal to -1 because $\sum_{u\in\mathbb{F}_\ell} w^u = 0$. $\square$

We now discuss applications. Let $a \in \mathbb{Z}$, and let $m = 4\,|a|$; then there exists a unique character modulo m such that, for all $p \nmid m$, $\chi_a(p) = \left(\frac{a}{p}\right)$. Uniqueness is obvious; next time, we will show existence from quadratic reciprocity.

§8 Day 8: (Sep. 25, 2025)

Today, we will talk about analytic continuations and an analytic function for ζ.

Theorem 8.1. $\zeta(s)$ is meromorphic on all of $\mathbb{C}$, with the only pole being at $s = 1$ (we already know that ζ is meromorphic for $\Re s > 0$).

Theorem 8.2 (Approximate Formulation)**.** We have that $\zeta(s) = \zeta(1-s)$ up to some simple factor for $0 < \Re s < 1$.

We have that the second theorem implies the first. If $\zeta(s)$ were just equal to $\zeta(1-s)$ for $0 < \Re s < 1$, we could define $\zeta(s)$ for $\Re(s) < 1$ as $\zeta(1-s)$.

Recall the Gamma function,

$$\Gamma(s) = \int_0^\infty t^{s-1} e^{-t}\, dt,$$

which converges absolutely for $\Re s > 0$. We can check that integrating on $\Re s > 0$ causes no problems, since

$$\int_\varepsilon^1 t^{s-1}\, dt = \frac{t^s}{s}\bigg|_\varepsilon^t = \frac{1}{s} - \frac{\varepsilon^s}{s}.$$

Lemma 8.3. $\Gamma(s)$ is absolutely convergent for $\Re s > 0$ and defines an analytic function. $\Gamma(s)$ is a continuous version of $n!$.

To do this, we have to show uniform convergence on a compact set.

Claim 8.4. (i) $\Gamma(s+1) = s\Gamma(s)$, (ii) $\Gamma(1) = 1$, (iii) $\Gamma(s)$ is meromorphic on all of $\mathbb{C}$ with simple poles at $0, -1, -2, \ldots$.

Together, we get $\Gamma(n) = (n-1)!$ for $n \in \mathbb{N}$, and observe that $\Gamma(s) = \frac{1}{s}\Gamma(s+1)$, which is meromorphic for $\Re s > -1$, with a simple pole at $s = 0$ (residue 1). In this manner, near $s = -1$, $\frac{\Gamma(s+1)}{s}$ has a simple pole at $s = -1$. We may proceed inductively to conclude the third part of the claim. We now check the first and second parts of the claim, where we first integrate by parts to get

$$\int_0^\infty t^{s-1} e^{-t}\, dt = \int_0^\infty \left(\frac{t^s}{s}\right)' e^{-t}\, dt - \int_0^\infty \frac{t^s}{s}(e^{-t})'\, dt = \int_0^\infty \frac{t^s}{s} e^{-t}\, dt = \frac{\Gamma(s+1)}{s}.$$

Also,

$$\Gamma(1) = \int_0^\infty e^{-t}\, dt = -e^{-s}\big|_0^\infty = 1.$$

As a fun fact, if we pick s, s', then we have that

$$\Gamma(s+s')B(s,s') = \Gamma(s)\Gamma(s'), \quad B(s,s') = \int_0^1 x^{s-1}(1-x)^{s'-1}\, dx.$$

With the above established (minus the part about B functions, that was just for fun), we have that $\xi(s) = \zeta(s)\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})$.

Theorem 8.5. $\xi(s) = \xi(1-s)$.

Proof. We check that

$$\zeta(s)\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right) = \zeta(1-s)\pi^{\frac{s-1}{2}}\Gamma\left(\frac{1-s}{2}\right).$$

Near $s = 0$, we have that $\zeta(s)$ is non-singular at $s = 0$, $\Gamma(\frac{s}{2})$ has a first order pole, $\zeta(1-s)$ has a first order pole at $s = 0$, and $\Gamma(\frac{1-s}{2})$ is non-singular.

As an example, if we let $s = -2$, $\zeta(s)$ will have a zero of first order, and $\zeta(s)$ will have simple zeros at even negative integers (i.e., the "trivial" zeros). This laeds into the Riemann hypothesis, i.e. that the only other zeros of ζ are on the line $\Re s = \frac{1}{2}$, which we call the "critical line". There is an axis of symmetry for $s \mapsto 1-s$. $\square$

Let $\theta(u)$ be the series,

$$\theta(u) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2 u} = 1 + 2(e^{-\pi n} + e^{-4\pi u} + e^{-9\pi u} + \dots).$$

We want to show that θ is absolutely convergent for $\Re u > 0$.

Claim 8.6. $\theta(\frac{1}{u}) = u^{\frac{1}{2}}\theta(u)$.

Our goal is to first formulate the Poisson summation formula and deduce the claim from it, then show that the claim demonstrats $\zeta(s) = \zeta(1-s)$. We start with the summation formula. Let $f : \mathbb{R} \to \mathbb{C}$ be a "nice function", i.e., f is infinitely differentiable and for all polynomials $p(x)$, we have that

$$\lim_{|x|\to\infty} \left| f(x)p^{(n)}(x) \right| = 0,$$

i.e., it is rapidly decreasing with all its derivatives. In fact, it is enough to require that f is C^2 with the rapidly decreasing condition up to its second derivative. As an example, take $f(x) = e^{-\pi u x^2}$ for $\Re u > 0$.

Definition 8.7 (Fourier Transform)**.** $\hat{f}(y) = \int_{-\infty}^{\infty} e^{2\pi i x y} f(x)\, dx$.

In particular, the Poisson summation formula is given by

$$\sum_{n=-\infty}^{\infty} f(n) = \sum_{n=-\infty}^{\infty} \hat{f}(n).$$

This means that we obtain $\theta(\frac{1}{u}) = n^{\frac{1}{2}}\theta(u)$, and by applying Poisson summation to $f(x) = e^{-\pi u x^2}$, we have $\hat{f}(y) =^{-\frac{1}{2}} e^{-\pi u^{-1} y^2}$, which follows from

$$\int_{-\infty}^{\infty} e^{-\pi u x^2}\, dx = u^{-\frac{1}{2}},$$

and

$$u^{-\frac{1}{2}}\theta\left(\frac{1}{2}\right) = u^{-\frac{1}{2}} \sum_{n=-\infty}^{\infty} e^{-\pi n^2 u^{-1}} = \sum_{n=-\infty}^{\infty} \hat{f}(n) = \sum_{n=-\infty}^{\infty} f(n) = \theta(u).$$

The Mellin transform also gives

$$2\xi(s) = \int_0^{\infty} (\theta(u) - 1) u^{\frac{s}{2}} \frac{du}{u},$$

and

$$\frac{\theta(u)-1}{2}=\sum_{n=1}^{\infty}e^{-\pi^2nu},$$

where we may let $t=\pi n^2u$ and $u^{\frac{s}{2}-1}=\frac{t^{\frac{s}{2}-1}}{(\pi n^2)^{\frac{s}{2}-1}}$. This means we obtain

$$\int_0^\infty e^{-\pi n^2u}u^{\frac{s}{2}-1}\,du=\left(\int e^{-t}t^{\frac{s}{2}-1}\,dt\right)=\frac{1}{(\pi n^2)^{\frac{s}{2}}}=\frac{1}{\pi^{\frac{s}{2}}n^s}.$$

Summing over all n, we have

$$\zeta(s)=\int_0^\infty\left(\frac{\theta(u)-1}{2}\right)u^{\frac{s}{2}}\,\frac{du}{u},$$

meaning we may identify ξ with ζ on its domain. We may further write

$$\int_0^\infty(\theta(u)-1)u^{\frac{s}{2}}\,\frac{du}{u}=\int_0^1+\int_1^\infty=-\frac{2}{s}+\int_0^1\theta(u)u^{\frac{s}{2}}\,\frac{du}{u}+\int_1^\infty(\theta(u)-1)u^{\frac{s}{2}}\,\frac{du}{u}.$$

Using

$$\begin{aligned}\int_0^1\theta(u)u^{\frac{s}{2}}\,\frac{du}{u}&=\int_1^\infty\theta(u^{-1})u^{-\frac{s}{2}}\,\frac{du}{u}\\&=\int_1^\infty\theta(u)u^{\frac{1-s}{2}}\,\frac{du}{u}\\&=\frac{2}{s-1}+\int_1^\infty(\theta(u)-1)u^{\frac{1-s}{2}}\,\frac{du}{u},\end{aligned}$$

we get that

$$\xi(s)+\frac{1}{s}+\frac{1}{1-s}=\frac{1}{2}\int_1^\infty(\theta(u)-1)u^{\frac{s}{2}}\,\frac{du}{u}+\frac{1}{2}\int_1^\infty(\theta(u)-1)u^{\frac{1-s}{2}}\,\frac{du}{u},$$

which is symmetric under $s\mapsto 1-s$, since ξ itself is symmetric as well.

§9 Day 9: Fourier Transform (Sep. 30, 2025)

Last time, we had

$$\xi(s) = \zeta(S)\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right), \quad \xi(s) = \xi(1-s),$$

and

$$f(x) = e^{-\pi ux^2} \implies \hat{f}(y) = u^{-\frac{1}{2}}e^{-\pi u^{-1}y^2}$$

from the Poisson summation formula, where if $f(x)$ is a "nice" function on $\mathbb{R}$, then

$$\hat{f}(y) = \int_{-\infty}^{\infty} e^{2\pi ixy} f(x)\, dx.$$

We expect that the more rapidly decreasing f is, the smoother $\hat{f}$ is, and vice versa. We have that $S(\mathbb{R}) \subset C^\infty(\mathbb{R})$; for every $f \in C^\infty(\mathbb{R})$, we have that $f \in S(\mathbb{R})$ as well if $(1+|x|^r)\left|f^{(i)}(x)\right|$ is bounded for all $r > 1$, $i \geq 0$; we note that $1+|x|^r$ can be replaced by any polynomial.

Theorem 9.1. $f \mapsto \hat{f}$ is an isomorphism from $S(\mathbb{R})$ to $S(\mathbb{R})$, where $\hat{f}(x) = f(-x)$.

Recall the Poisson summation; for all $f \in S(\mathbb{R})$, we have that

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n).$$

Consider a function on $\mathbb{R}/\mathbb{Z}$ (i.e., $\mathbb{Z}$-periodic function on $\mathbb{R}$), where f is any "nice" function (such as continuous); then its Fourier series coefficients is given by

$$a_n = \int_0^1 f(x)e^{-2\pi inx}\, dx = \int_{\mathbb{R}/\mathbb{Z}} \dots,$$

and the series itself is $\sum a_n e^{2\pi inx}$. If f is "nice", the Fourier series converges in the original function. Said "nice" functions define the inner product

$$\langle f, g\rangle = \int_0^1 f(x)\overline{g(x)}\, dx,$$

where $\{e^{2\pi inx}\}$ is an orthonormal basis.

Theorem 9.2. If f is C^2 and $\mathbb{Z}$-periodic, then $f(x) = \sum_{n\in\mathbb{Z}} a_n e^{2\pi inx}$ is absolutely convergent.

Let $f \in S(\mathbb{R})$; we have that $F(x) = \sum_{n\in\mathbb{Z}} f(x+n)$ is a C^∞ function on $\mathbb{R}/\mathbb{Z}$, so $F(0) = \sum_{n\in\mathbb{Z}} f(n)$ is just the sum of Fourier coefficients $\sum_{n\in\mathbb{Z}} a_n = \sum_{n=-\infty}^{\infty} \int_0^1 e^{2\pi inx} F(x)\, dx$. This yields

$$\sum_{n,m\in\mathbb{Z}} \int_0^1 e^{2\pi inx} f(x+m)\, dx,$$

so if we fix n, we have that

$$\sum_{m\in\mathbb{Z}} \int_0^1 e^{2\pi inx} f(x+m)\, dx = \sum_{m\in\mathbb{Z}} \int_m^{m+1} e^{2\pi inx} f(x)\, dx = \int_{-\infty}^{\infty} e^{2\pi inx} f(x)\, dx = \hat{f}(n).$$

It is enough to require that there exists some $x > 1$ such that

$$(1+|x|^n)(|f| + |f''|)$$

is bounded, and $f \in C^2$. We may prove this differently, however; consider $S(\mathbb{R})$ as a vector space, and define $S^*(\mathbb{R})$ as a tempered distribution of linear functional on $S(\mathbb{R})$ which are continuous in some sense. Then $f \mapsto \sum_{n\in\mathbb{Z}} f(n)$ is an element of $S^*(\mathbb{R})$. Observe that $\lambda(f(x+n)) = \lambda(f)$ for all $n \in \mathbb{Z}$; then

$$\lambda(e^{2\pi inx} f(x)) = \lambda(f(x)), \quad n \in \mathbb{Z}.$$

Lemma 9.3. An element of $S^*(\mathbb{R})$ with these properties is unique up to multiplication by a constant.

On the other hand, $\mu(f) = \sum_{n\in\mathbb{Z}} \hat{f}(n)$, so we claim that μ satisfies the same properties; λ is equal to μ up to a constant, so we show that the constant is equal to 1. It is enough to find f such that $\lambda(f) = 0$ and $f = \hat{f}$. If we take $f(x) = e^{-\pi x^2}$, we have that

$$\widehat{e^{2\pi imx} f}(x) = \int_{-\infty}^{\infty} e^{2\pi ixy} e^{2\pi imx} f(x)\, dx = \int_{-\infty}^{\infty} e^{2\pi ix(y+m)} f(x)\, dx = \hat{f}(y+m).$$

We have that the correction function in the definition of $\xi(s)$ can be written as

$$\int_0^{\infty} e^{-\pi x^2} x^{s-1}\, dx.$$

§10 Day 10: Norms and Integration on $\mathbb{Q}^p$ (Oct. 2, 2025)

We want to motivate the correction factor; start by computing the following with the change of variables $y = \pi x^2$,

$$\begin{aligned}\int_0^\infty e^{-\pi x^2} x^{s-1}\, ds &= \frac{1}{2}\int_0^\infty e^{-y}\left(\frac{y}{\pi}\right)^{\frac{s-1}{2}}\left(\frac{y}{\pi}\right)^{-\frac{1}{2}}\frac{1}{\pi}\, dy \\ &= \frac{1}{2}\int_0^\infty e^{-y} g^{\frac{s}{2}-1}\pi^{1-\frac{s}{2}}\frac{1}{\pi}\, dy = \frac{1}{2}\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right).\end{aligned}$$

This means we have

$$\int_0^\infty e^{-\pi x^2}|x|^{s-1}\, dx = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right) = \int_{-\infty}^\infty e^{-\pi x^2}|x|^2\frac{dx}{|x|}.$$

Recall that if K is any field, we define a norm on K to be a map $\|\cdot\| : K \to \mathbb{R}_{\geq 0}$ such that it is absolutely homogeneous, subadditive, and equal to 0 if and only if the input is zero. For example,

(i) $\mathbb{R}$ or $\mathbb{C}$ with the usual absolute value and "Euclidean distance from origin" norm,

(ii) (*p-adic norm*) $K = \mathbb{Q}$; any element of $\mathbb{Q}$ can be written as $\frac{p^s r}{q}$, where p is prime and $p \nmid r$. Then the norm of such is given by p^{-s} (we also define the norm of 0 to be 0 in this case).

We know that norms induce metric topologies on the space that is being normed, and we say that two norms are equivalent if they induce the same topology.

Exercise 10.1. Two norms $\|\cdot\|_1, \|\cdot\|_2$ are equivalent if and only if there exists c such that $\|\cdot\|_1 = \|\cdot\|_2^c$.

Theorem 10.2 (Ostrowski)**.** For $K = \mathbb{Q}$, the usual norm and the p-adic norm are the only norms for K up to equivalence. We say that the p-adic norm is *archimedean*, and the usual norm *non-archimedean*.

If K is a field with norm $\|\cdot\|$, you can do the following;

(i) You can define the convergence of a sequence and its limits.

(ii) You can take Cauchy sequences.

$\mathbb{Q}$ is not complete with respect to the p-adic norm nor the usual 2-norm, so Cauchy sequences do not necessarily converge here. In general, if K is a normed field, we can define its completion $\hat{K}$ with respect to the original norm. Elements of $\hat{K}$ are Cauchy sequences up to e.quivalence, i.e., $\{a_n\}$ is Cauchy if, for all $\varepsilon > 0$, there exists $N > 0$ such that $|a_n - a_m| < \varepsilon$ for all $n, m \geq N$. We say that $\{a_n\} \sim \{k_n\}$ if, for all $\varepsilon > 0$, there exists N such that $|a_n - k_m| < \varepsilon$ for all $n, m \geq N$. Cauchy sequences up to equivalence form a field containing K, but is complete, which we call $\hat{K}$.

As an example, take $K = \mathbb{Q}$ with th eusual notion; then $\hat{K} = \mathbb{R}$. Let p be prime, and let $\mathbb{Q}_p$ be defined as the completion of $\mathbb{Q}$ with resepect to $\|\cdot\|_p$; then $\mathbb{Z}_p \subset \mathbb{Q}_p$, where $\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ inside $\mathbb{Q}_p$. The *explicit* definition of Z_p is that we have

$$\mathbb{Z}_p = \lim_{n\to\infty}\mathbb{Z}/p^n\mathbb{Z} = \{a_n \in \mathbb{Z}/p^n\mathbb{Z} \mid a_n \text{ is the image of } a_{n+1} \text{ under } \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}\}.$$

Since this is a ring, addition and multiplication are defined as term-by-term addition and multiplication of $\{a_n\}$.

Lemma 10.3. Any Cauchy sequence of integers with respect to $\|\cdot\|_p$ converges in $\mathbb{Z}_p$ and any element of $\mathbb{Z}_p$, and any element of $\mathbb{Z}_p$ is a limit of integers.

Let $|\{a_n\}| = p^{-(m-1)}$, i.e., m is the smallest integer where $a_m \neq 0$; then we see that $\mathbb{Q}_p$ is the field of fractions of $\mathbb{Z}_p$, where $\mathbb{Q}_p \ni x = \frac{a}{b}$ and $a_1 b \in \mathbb{Z}_p$? In fact, any element of $\mathbb{Q}_p$ has the form $\frac{a}{p^\ell}$, where $a \in \mathbb{Z}_p$ and $\ell \geq 0$.

We now discuss integration on $\mathbb{Q}_p$. Let $S(\mathbb{Q}_p)$ be the set of locally constant complex-valued functions with compact support on $\mathbb{Q}_p$. Since $\mathbb{Z}_p \subset \mathbb{Q}_p$, we may write the following lemma,

Lemma 10.4. $\mathbb{Z}_p$ is open and compact in $\mathbb{Q}_p$.

Let $f : \mathbb{Q}_p \to \mathbb{C}$ have bounded support. If there exists $p > 0$ such that $f(x) = 0$ if $|x| \geq r$, then f is locally constant, i.e., every point has a neighborhood such that f is constant on said neighborhood. We also have that f has compact support if and only if there exists $n \geq 0$ such that $f(x+y) = f(x)$ for all $x, y \in p^n\mathbb{Z}_p$. We call $S(\mathbb{Q}_p)$ the space of *Schwartz-Bruhat* functions.

If $f \in S(\mathbb{Q}_p)$, we can define $\int_{\mathbb{Q}_p} f(x)\,dx$. Assume, for example, that the support of f is in $\mathbb{Z}_p$. Then $f(x) = 0$ if $x \notin \mathbb{Z}_p$, and there exists n such that $f(x+y) = f(x)$ for all $z \in p^n\mathbb{Z}_p$, since $\mathbb{Z}_p/p^n\mathbb{Z}_p = \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{C}$ under $\overline{f}$. Define

$$\int_{\mathbb{Z}_p} f(x)\,dx = p^{-n} \sum_{a \in \mathbb{Z}/p^n\mathbb{Z}} \overline{f}(a).$$

For $\int_{\mathbb{Q}_p}$, note that $\mathbb{Q}_p/p^n\mathbb{Z}_p = \mathbb{Q}/p^n\mathbb{Z}$, so any $f \in S(\mathbb{Q}_p)$ is actually a function $\overline{f}$ on $\mathbb{Q}/p^n\mathbb{Z}$, with finite support. Then define the integral by the same formula. As an example,

$$\int_{\mathbb{Z}_p} 1\,dx = 1 = \int_{\mathbb{Z}_p} f(x)\,dx, \quad f(x) = \begin{cases} 1 & |x| \leq 1, \\ 0 & |x| > 1, \end{cases} \quad f_n(x) = \begin{cases} 1 & |x| \leq p^{-n}, \\ 0 & |x| > p^{-n}. \end{cases}$$

In this manner, we analogously obtain $\int_{\mathbb{Q}_p} f_n(x)\,dx = p^{-n}$. Observe that

$$\int_{\mathbb{Q}_p} f_n(x)\,|x|^s\,dx = \int_{\mathbb{Z}_p} |x|^s\,dx,$$

even though we are "cheating" a little bit because $|x|^s$ is not an element of $S(\mathbb{Q}_p)$; really, we are writing

$$\int_{\mathbb{Z}_p} |x|^s\,dx = \sum_{n \geq 0} \int_{|x|=p^{-n}} p^{-ns}\,ds;$$

we claim that $\int_{|x|=p^{-n}} 1\,dx = (p-1)p^{-(n+1)}$. For $n = 0$, we have that $\{x \mid |x| = 1\} = \mathbb{Z}_p \setminus p\mathbb{Z}_p$, and consider the map $\pi : \mathbb{Z}_p \to \mathbb{Z}/p\mathbb{Z}$ and $\{x \mid |x| = 1\} \mapsto (\mathbb{Z}/p\mathbb{Z})^*$. Assume that $\pi^{-1}(a)$ has volume p^{-1}. Altogether, we get $(p-1)p^{-1}$. For other n, the calculation is similar.

In this manner, consider

$$\int_{\mathbb{Q}_p} f_0(x)\,|x|^{s-1}\,dx = \sum_{n \geq 0} p^{-n(s-1)}(p-1)p^{-(n+1)} = \frac{p-1}{p} \sum_{n \geq 0} p^{-ns} = \frac{p-1}{p} \frac{1}{1-p^{-s}},$$

where we recognize the latter fraction as the Euler factor in the Riemann ζ-function. Specifically,

$$\Gamma\left(\frac{s}{2}\right) n^{-\frac{s}{2}} = \int_0^\infty e^{-\pi x^2} (x)^{s-1}\,dx,$$

where we recall the definition of f_0. The analog of $e^{-\pi/s^2}$ is $f_0(x)$ up to a constant. $e^{-\pi s^2}$ is essetnailly the simplest possible function whose Fourier transform is closed. $f_n(x)$ has a similar property of $\mathbb{Q}_p$, where $s \mapsto e^{2\pi i x}$ is a homomorphism from $\mathbb{R}$ to $\mathbb{C}^*$. Recall that the Fourier transform is given by

$$\hat{f}(y) = \int_{\mathbb{R}} f(x) e^{2\pi i x y} \, dx.$$

We want an continuous additive character of $\mathbb{Q}_p$. Take a character $\psi : \mathbb{Q}_p/\mathbb{Z}_p \to \mathbb{C}^*$, where $\mathbb{Q}_p/\mathbb{Z}_p = \{a \in \mathbb{Q}/\mathbb{Z} \mid ap^i = 0, i >> 0\}$; then

$$0 \subset p^{-1}\mathbb{Z}/\mathbb{Z} \subset p^{-2}\mathbb{Z}/\mathbb{Z} \subset p^{-3}\mathbb{Z}/\mathbb{Z} \subset \dots.$$

We may pick any additive character φ such that $\psi|_{p^{-1}\mathbb{Z}/\mathbb{Z}} \neq 1$ as the analog of $e^{2\pi i x}$. In this manner, we have that

$$\hat{f}(y) = \int_{x \in \mathbb{Q}_p} f(x) \psi(x, y) \, dx.$$

Lemma 10.5. If $f \in S(\mathbb{Q}_p)$, then $\hat{f}(y) = S(\mathbb{Q}_p)$. We also have that $\hat{f}(x) = f(-x)$.

$f = f_0$ is the characteristic function of $\mathbb{Z}_p \subset \mathbb{Q}_p$. We have that $\hat{f_s}(0) = f_s(y)$, and for $y \in \mathbb{Z}_p$, we have

$$\hat{f_0}(y) = \int_{z \in \mathbb{Q}_p} f_0(x) \psi(xy) \, dx = \int_{\mathbb{Z}_p} \psi(xy) \, dx = \int_{\mathbb{Z}_p} 1 \, dx.$$

In particular, since for any $z, y \in \mathbb{Z}_p$, we have $xy \in \mathbb{Z}_p$, we have that $\psi(xy) = 1$. If $x \notin \mathbb{Z}_p$, then $x \mapsto \psi(xy)$ is a nontrivial character of $\mathbb{Z}_p$, and

$$\int_{\mathbb{Z}_p} f_y(x) \, dx = p^{-n} \sum_{a \in \mathbb{Z}/p^n\mathbb{Z}} \overline{\psi}_y(a) = 0.$$

We may choose n such that $\psi_y(x)$ is trivial on $p^n\mathbb{Z}_p$, and so $\psi_y(x)$ can be regarded as a nontrivial function $\overline{\psi}_y$ on $\mathbb{Z}/p^n\mathbb{Z}$.

§12 Day 12: Proof of Prime Number Theorem (Oct. 9, 2025)

Today we will give a proof of the prime number theorem, probably modulo the "analytic theorem". Let $\pi(x)$ be the prime counting function denoting the number of primes less than or equal to x; we want to show that

$$\pi(x) \sim \frac{x}{\log x},$$

with the limit of this ratio approaching 1 as $x \to \infty$. Recall from last time that we have the following functions defined,

$$\zeta(s) = \sum_n \frac{1}{n^s}, \quad \Phi(s) = \sum_p \frac{\log p}{p^s}, \quad \theta(x) = \sum_{p \le x} \log p.$$

Last time, we proved that the prime number theorem follows from the fact that $\theta(x) \sim x$, i.e.,

$$\lim_{x\to\infty} \frac{\theta(x)}{x} = 1,$$

which was obtained from writing

$$(1-\varepsilon)\log x \cdot \big(\pi(x) + O(x^{1-\varepsilon})\big) \le \theta(x) \le \pi(x)\log x,$$

for which we may divide throughout by $\log x$ and take $x \to \infty$ to get the desired result. The first step towards this proof is to check that

$$\int_1^\infty \frac{\theta(x) - x}{x^2}\, dx$$

is convergent; assuming $\lim_{x\to\infty} \frac{\theta(x)}{x} \neq 1$, there exists some arbitrarily large x such that $\theta(x) \ge \lambda x$, or there exists $\lambda < 1$ such that for arbitrarily large x, $\theta(x) \le \lambda x$. Supposing the former case occurs for some x; we have that

$$\int_x^{\lambda x} \frac{\theta(t) - t}{t^2}\, dt \ge \int_x^{\lambda x} \frac{\lambda x - t}{t^2}\, dt = \int_1^\lambda \frac{\lambda - \tau}{\tau^2}\, d\tau > 0$$

obtained by picking $\tau = xt$. Observe that, if for some f, we have that $\int_1^\infty f(t)\, dt$ is convergent, then for all $\varepsilon > 0$, there exists A such that $\left|\int_a^b f(t)\, dt\right| < \varepsilon$ for $A \le a \le b$. Thus, pick $f(t)$ to be our integrand as above, and we have that if $\int_1^\lambda \frac{\lambda-\tau}{\tau^2}\, d\tau > \varepsilon$, we have a contradiction. In the latter case, we have that

$$\int_{\lambda x}^\lambda \frac{\theta(t) - t}{t^2}\, dt \le \int_{\lambda x}^x \frac{\lambda x - t}{t^2}\, dt = \int_\lambda^1 \frac{\lambda - t}{t^2} < 0,$$

and we may apply the same argument. Returning to the original statement, we see that convergence of $\int \frac{\theta(x)-x}{x^2}\, dx$ follows from (i) the observation that $\frac{\theta(x)}{x}$ is bounded, since $\theta(x) = O(x)$, (ii) that $\Phi(s)$ is holomorphic on $\Re s \ge 1$ (as it has no zeroes on this set), (iii) the "tauberian" theorem, i.e., $f(t)$ is a bounded, locally integrable function defined for $t \ge 0$; taking $g(z) = \int_0^\infty f(t) e^{-zt}\, dt$, which is holomorphic for $\Re z > 0$, and assuming that it is holomorphic on $\Re z \ge 0$, we have that $g(0) = \int_0^\infty f(t)\, dt$, and that the RHS is convergent.

To prove the convergence of the integral, it suffices to prove (ii) and (iii), since (i) was proved last time.

Theorem 12.1 (Classical Tauberian theorem)**.** Let $\{a_n\}$ be a sequence such that $a_n = o(\frac{1}{n})$ if and only if $\lim_{n\to\infty} na_n = 0$, i.e., a_n goes to 0 slightly better than $\frac{1}{n}$. Then $f(x) = \sum a_n x^n$ is holomorphic for $|z| < 1$, and we may assume that $\lim_{|z|<1, z\to 1} f(x)$ exists and is equal to s. Then $\sum_{k=0}^{\infty} a_n = s$.

We have that $\Phi(s)$ is absolutely convergent for $\Re s > 1$ (uniformly on compact sets); for all $\varepsilon > 0$, we have that $\log < x^2$ for $x \gg 0$. For $p \gg 0$, we also have that

$$\left|\frac{\log p}{p^s}\right| = \left|\frac{p^\varepsilon}{p^s}\right| = \left|\frac{1}{p^{s-\varepsilon}}\right|.$$

If $\Re s > 1$, find $\varepsilon > 0$ such that $\Re(s-\varepsilon) > 1$; the above implies that $\sum_{n=1}^{\infty} \frac{1}{n^{s-\varepsilon}}$ is absolutely convergent, and so $\sum \frac{1}{p^{s-\varepsilon}}$ also converges, and so $\sum \frac{\log p}{p^2}$ is also convergent. Directly write as follows,

$$\sum_p \frac{\log p}{p^s} = \int_1^\infty \frac{d\theta(x)}{x^s} = \int_1^\infty \frac{\theta(x)}{x^{s+1}}\,dx = \sum_{i=0}^{\infty} s\int_{p_i}^{p_{i+1}} \frac{\theta(x)}{x^{s+1}}\,dx = \sum_{i=1}^{\infty} (p_i^{-s} - p_{i+1}^{-s})\theta(p_i).$$

Thus, $\Phi(s) = \sum p_i^{-s}\log p_i$. We may also write $\Phi(s) = s\int_0^\infty e^{-st}\theta(e^t)\,dt$, so taking $f(t) = \theta(e^t)e^{-t} - 1$, observe the following lemma,

Lemma 12.2. $g(z) = \frac{\Phi(z+1)}{z+1} = \frac{1}{z}$.

$$\int_0^\infty f(t)x^{-st}\,dt = \int_0^\infty \theta(e^t)e^{-t}e^{-st}\,dt - \int e^{-zt}\,dt = \frac{\phi(z+1)}{z+1} - \frac{1}{z},$$

which is holomorphic for $\Re z \geq 0$. Observe that our three observations from earlier are that (i) $\theta(s) = O(s)$ guarantees boundedness for $f(t)$, (ii) guarantees the assumption in the theorem, and (iii) shows that the theorem is equivalent to the convergence of our integral.

We now discuss the analyticity of $\Phi(x)$ and its connection to the absence of zeroes of $\zeta(s)$. Observe that we have

$$\log(\zeta(s))' = \frac{\zeta'(s)}{\zeta(s)} = \sum_p \frac{\log p}{p^2 - 1} = \Phi(s) + \sum_p \frac{\log p}{p^s(p^s-1)}.$$

Also, the sum converges for $\Re s > \frac{1}{2}$. The above shows that $\Phi(s)$ is meromorphic for $\Re s > \frac{1}{2}$, and we want to see that its only simple pole is at $s = 1$. Moreover, poles of $\Phi(s)$ for $\Re s > \frac{1}{2}$ are poles of $\zeta'(s)/\zeta(s)$, so it is enough to show that $\zeta(s)$ has no zeroes for $\Re s = 1$, since we've already established previously that it has no zeroes for $\Re s > 1$.

Assume we have a zero of order μ of ζ at $1 + i\alpha$. Then we also have the same at $1 - i\alpha$. Let ν be the order of the zero of ζ at $1 + 2i\alpha$. Then

$$\sum_{\nu=-2}^{2} \binom{4}{2+r} \phi(1+\varepsilon+i\nu\alpha) = \sum_p \frac{\log p}{p^{1+\varepsilon}}\left(p^{i\alpha/2} + p^{-i\alpha/2}\right)^4 \geq 0.$$

Some quick computations follow that $\mu = 0$, since $6 - 8p - 2\nu \geq 0$.[1]

[1] sloppy writing this time, i'm tired as heck

§13 Day 13: (Oct. 14, 2025)

We digress the course a little bit; we want to do some analytic number theory related to general number fields. Today, we will study what "prime" means in more general number fields.

Let $\overline{\mathbb{Q}}$ be the field of algebraic numbers; observe that we have $\mathbb{Q} \subset \overline{\mathbb{Q}} \subset \mathbb{C}$, where we have that $\alpha \in \mathbb{C}$ is algebraic (over $\mathbb{Q}$) if there exists $f(x) \in \mathbb{Q}[x]$ with $f(x) = 0$ such that $f(\alpha) = 0$. Equivalently, the field $K = \mathbb{Q}(\alpha) \subset \mathbb{C}$ is a finite extension of $\mathbb{Q}$, i.e., $\dim_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ is finite. In general, if $L \supset K$ as fields, we say that the degree of the extension $[L : K] = \dim_K L$, where we say that L is a finite extension if $[L : K] < \infty$.

Fact 13.1. The algebraic numbers form a field.

Definition 13.2. A number field K is a subfield of $\mathbb{C}$ which is a finite extension of $\mathbb{Q}$.

We give a few examples; (i) $K = \mathbb{Q}$ is trivially a number field, (ii) $\mathbb{Q}(i) = \{a+bi \mid a, b \in \mathbb{Q}\}$ has $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, (iii) $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$. For $K = \mathbb{Q}$, we also have $\mathbb{Z}$ as the ring of integers, and we may regard the positive integers as non-zero ideals of $\mathbb{Z}$. Given a commutative ring R, $I \subset R$ is an ideal if it is closed under addition, and for all $i \in I$, $R \ni a \mapsto ai \in I$. I is called a principal ideal if there exists $i \in R$ such that $I = \{ai \mid a \in R\}$.

Fact 13.3. Any ideal of $\mathbb{Z}$ is principal.

Clearly, $\langle i \rangle = \langle -i \rangle$, and we have that $\langle i \rangle = \langle j \rangle$ implies $i = \pm j$ for $\mathbb{Z}$, and in general for any ring R, it means that there exists $u \in R^*$ (regarded as the group of invertible elements in R) such that $i = uj$. Since R has no zero divisors, it is an integral domain. For $\mathbb{Z}$, we have a unique decomposition into product of primes, and only in $\mathbb{Z}$ do we have a unique decomposition into a product of primes up to sign. (?)

We now discuss the ring of integers of a number field. $\alpha \in \overline{\mathbb{Q}}$ is an algebraic niteger if there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. Specifically, this is equivalent to $\mathbb{Z}[\alpha] \subset \mathbb{C}$ being a finitely generated abelian group, which is equivalent to it being a finitely generated $\mathbb{Z}$-module.

Exercise 13.4. Prove that the algebraic integers form a subring of $\overline{\mathbb{Q}}$.

Let K be a number field, i.e., a finite extension of $\mathbb{Q}$. Let $\mathcal{O}_K$ be the ring of integers of K. We have that $\mathcal{O}_K$ is given by the intersection of the algebraic integers and K. As some examples, if $K = \mathbb{Q}(i)$, then $\mathcal{O}_K = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. For $K = \mathbb{Q}(\sqrt{5})$, we have that $\mathcal{O}_K = \mathbb{Z}[\frac{1 \pm \sqrt{5}}{2}]$.

We want to develop some sort of "arithmetic" system for $\mathcal{O}_K$ similar to the usual arithmetic for $\mathbb{Z}$. As another example, consider $K = \mathbb{Q}(\sqrt{-5})$. We can show that $2 + \sqrt{-5}$ is a unit.

Given R a ring and $p \subset R$ an ideal, we say that p is prime if R/P is an integral domain (has no zero divisors). Next lecture, we will give a more correct analog of the idea that prime numbers are prime ideals of $\mathcal{O}_K$.

§14 Day 14: Field Extensions (Oct. 16, 2025)

Last time, we discussed that $K \subset \mathbb{C}$ is a number field if and only if it is a finite extension of $\mathbb{Q}$, and $K \supset \mathcal{O}_K$ (the ring of integers), where we can think of $\mathcal{O}_K$ as the intersection of the algebraic integers (recall that this is the set of all α such that there exists $f \in \mathbb{Z}[x]$ with $f(\alpha) = 0$) and K.

Let E/F be a finite extension of fields, where $\dim_F E < \infty$. We define a norm $N_{E/F} : E \to F$ to be given by

$$N_{E/F}(xy) = N_{E/F}(x)N_{E/F}(y),$$

where $N_{E/F}(x)$ is the determinant of the multiplication map by x as a map from F to E. We denote $\mathrm{Tr}_{E/F}$ as the trace of the same map. Assume E, F both have characteristic zero (more generally, we need E/F to be a separable extension); let $E(x)$ be the minimal polynomial of α. Then the monic polynomial of minimal degree in $F[x]$ such that $f(\alpha) = 0$,

$$f(x) = x^m + \sum_{i=0}^{m} -1 a_i x^i.$$

is the minimal polynomial for the map of multiplication by α from F to E.

Claim 14.1. *n is divisible by m, and $N_{E/F}(\alpha) = [(-1)^m a_n)]^{n/m}$, i.e., the product of all roots of f with multiplicity n/m.*

We have that $E \supset F(\alpha) \supset F$, and $[E : F] = [E : F(\alpha)] \cdot [F(\alpha) : F]$.

Corollary 14.2. *$K = \mathbb{R}/\mathbb{Q}$ is a number field, and we have $\alpha \in \mathcal{O}_K$ implies $N_{E/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.*

Proof. This will follow if we know that the minimal polynomial of α is in $\mathbb{Z}[x]$. Let $f(x)$ be some monic polynomial in $\mathbb{Z}[x]$ such that $f(\alpha) = 0$, and let $f_{\min}(x)$ be the minimal polynomial of α over $\mathbb{Q}$. Then

$$f(x) = g(x) f_{\min}(x),$$

where $f(x) \in \mathbb{Z}[x]$ and $g, f_{\min} \in \mathbb{Q}[x]$. Assume that there exists some prime p such that some denominator of a coefficient of $f_{\min}$ is divisible by p. Let n be the max degree of p, for which all denominators of $p^n f_{\min}$ is prime to p, and at least one numerator is prime to p. We may do the same to g to get $p^m g$ with the same property. Now, we may reduce mod p, i.e., for any $a/b \in \mathbb{Q}$ with $(b, p) = 1$, we have that $(a \bmod p)(b \bmod p)^{-1} \in \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ as a field. Denote $\bar{\cdot}$ as the reduction; we may write

$$p^{n+m} f = (p^m g) \cdot (p^n f_{\min}) \implies 0 = \overline{p^m g} \cdot \overline{p^n f_{\min}} \in \mathbb{F}_p[x],$$

where both terms vanish under reduction. □

Definition 14.3. Let V be a vector space over $\mathbb{Q}$ of dimension n. A lattice $L \subset V$ is an abelian subgroup isomorphic to $\mathbb{Z}^n$. L has the form $L = \{\sum a_i v_i \mid a_i \in \mathbb{Z}\}$, where $\{v_i\}$ is some basis of V.

Lemma 14.4. *Let $L \subset V$ be a subgroup which spans V. Then the following are equivalent, (i) L is a lattice, (ii) L is finitely generated, and (iii) If $v_1, \ldots, v_n \in L$ is a basis of V, then there exists $\varepsilon > 0$ such that if $\sum a_i v_i \in L$, then for all i, either $a_i = 0$ or $|a_i| \geq \varepsilon$.*

Proof. Left as an exercise. □

Corollary 14.5. $\mathcal{O}_K \subset K$ is a lattice.

Proof. If $\alpha \in K$, then there exists nonzero $\beta \in \mathbb{Z}$ such that $p := \beta\alpha \in \mathcal{O}_K$. Let $f \in \mathbb{Q}[x]$ be monic such that $f(\alpha) = 0$; we may write

$$f(\alpha) = \alpha^n + \sum_{i=0}^{n-1} a_i \alpha^i = 0 \implies \left(\frac{p}{b}\right)^n + \sum_{i=1}^{n-1} a_i \left(\frac{p}{b}\right)^i = 0,$$

i.e., $p^n + \sum_{i=0}^{n-1} a_i b^{n-i} p^i = 0$, and we just need to find b such that $a_j b^{n-i} \in \mathbb{Z}$ for $i = 0, \ldots, n-1$. Let $v_1, \ldots, v_k$ be a basis of K over $\mathbb{Q}$ such that $v_i \in \mathcal{O}_K$ for all i. If $\sum a_i v_i \in \mathcal{O}_K$, then

$$N_{K/\mathbb{R}}\left(\sum_i a_i v_i\right) \in \mathbb{Z},$$

and if there exists $\sum a_i v_i \in \mathcal{O}_K$ (regarded as a homogeneous polynomial in a_i), with arbitrarily small a_i, then $N(\sum a_i v_I)$ is also arbitrarily small. $\square$

Corollary 14.6. Let $\alpha \in \mathcal{O}_K$. Then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$, i.e., the trace but for all coefficients of the characteristic polynomial of multiplication by α.

Proof. We can find $K \cong \mathbb{Q}^n$ such that $\mathcal{O}_K \cong \mathbb{Z}^n$ such that multiplication by α preserves $\mathcal{O}_K$, represented by an integral matrix. Thus, there indeed is an integral characteristic polynomial. Conversely, we also have that if the characteristic polynomial of $*\alpha$ is in $\mathbb{Z}[x]$, then $\alpha \in \mathcal{O}_K$. Fix a monic $f(x) \in \mathbb{Z}[x]$. Since $\alpha \in \mathcal{O}_K$, we have that $f(\alpha) = 0$ by linear algebra. $\square$

Corollary 14.7. Let α be a squarefree integer. Let $K = \mathbb{Q}(\sqrt{\alpha})$, so $[K : \mathbb{Q}] = 2$. We have that $\alpha \in \mathbb{Q}(\sqrt{d})$ is in $\mathcal{O}_K$ if and only if the norm and trace of α are in $\mathbb{Z}$.

Proof. Observe that $N_{K/\mathbb{Q}}(\alpha) = \alpha\overline{\alpha} = a^2 - b^2 d$, where we let $\alpha = a + b\sqrt{d}$ and $\overline{\alpha} = a - b\sqrt{d}$ (we note that $\alpha + \overline{\alpha}$ is the trace). Then $1, \sqrt{d}$ forms a basis of K over $\mathbb{Q}$. Multiplication by α is of the matrix

$$\begin{pmatrix} a & bd \\ b & a \end{pmatrix},$$

with determinant $a^2 - b^2 d$ and trace $2a$. $\square$

As an example, let $d = -1$; let $K = \mathbb{Q}(i)$, and consider that $a + bi \in \mathcal{O}_K$ if and only if $2\alpha \in \mathbb{Z}$, $a^2 + b^2 \in \mathbb{Z}$.

Lemma 14.8. Let $d \in \mathbb{Z}$ be squarefree. Then if $d \equiv 2, 3 \bmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$; if $d \equiv 1 \bmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, where we write $\alpha = \frac{1+\sqrt{d}}{2}$, and we have $\alpha^2 - \alpha = 0$.

We now do some counterexamples. Let $u \in \mathcal{O}_K$ be nonzero; we say u is a unit if $u \in \mathcal{O}_K^*$, i.e., $u^{-1} \in \mathcal{O}_K$.

Lemma 14.9. u is invertible if and only if $N_{K/\mathbb{Q}}(u) = \pm 1$.

Proof. $N(u^{-1}) = N(u)^{-1}$ implies $u \in \mathcal{O}_K^*$; then $N(u) \in \mathbb{Z}^*$. $\square$

Claim 14.10. Let $A \in M(n \times n, \mathbb{Z})$, and $\det A = \pm 1$. Then $A^{-1} \in M(n \times n, \mathbb{Z})$.

Proof. We have that $K \cong \mathbb{Q}^n \sup \mathbb{Z}^n \cong \mathcal{O}_K$, so if $N(u) = \pm 1$, we have that multiplication by u in this basis is a matrix in $M(n \times n, \mathbb{Z})$, and $u^{-1}\alpha \in \mathcal{O}_K$ if $u \in \mathcal{O}_K$. Take $\alpha = 1$. $\square$

As an example, consider $K = \mathbb{Q}(i)$. Then $\mathcal{O}_K = \mathbb{Z}[i]$, and $N(a+bi) = a^2 + b^2$. We have $\pm 1, \pm i$ as units. $\alpha \in \mathcal{O}_K$ is irreducible if, for all $\alpha = p_1 p_2$ with $p_1, p_2 \in \mathcal{O}_K$, we have p_1 or p_2 as a unit. It is true (and easy) to see that any nonzero $\alpha \in \mathcal{O}_K$ is a product of irreducible elements. The question is; is it unique? We can guess that the representation is unique up to multiplication by units and permutation; however, we see that this is still not true in general, by observing the example $\mathbb{Q}(\sqrt{-5}) = K \supset \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, where $\alpha = 6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$. We may check that all $a + b\sqrt{-5}$ is irreducible, since $N(a+b\sqrt{-5}) = a^2 + 5b^2$ (and a bunch more computations here and there that I didn't follow).

§15 Day 15: (Oct. 21, 2025)

Last class, we discussed that, given a number field K and a ring of integers $\mathcal{O}_K$, some examples of a non-principal ideal in $\mathcal{O}_K$. Let R be a ring, and let $\mathfrak{a} \subset R$ be an ideal; we say that it is principal if there exists some $\alpha \in R$ such that $\mathfrak{a} = \{x\alpha \mid x \in R\}$. If $\mathfrak{a} = (\alpha_1, \dots, \alpha_n)$, we have that $\mathfrak{a} = \{\sum_i x_i \alpha_i \mid x_i \in R\}$.

As an example, let $K = \mathbb{Q}(\sqrt{-5})$. We have that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, where we have the ideal $\mathfrak{a} = (2, 1 + \sqrt{-5})$, for which we observe is non-principal. Indeed, if $\mathfrak{a} = (\alpha)$, then $2 = \alpha x$ and $1 + \sqrt{-5} = \alpha y$; since $4 = N(2) = N(\alpha)N(x)$ and $6 = N(1 + \sqrt{-5}) = N(\alpha)N(y)$, we have that $N(\alpha)$ divides both 4 and 6, where $N(\alpha) \neq \pm 1$. Supposing $N(\alpha) = \pm 2$, we also obtain a contradiction since

$$\alpha = a + b\sqrt{-5} \implies N(\alpha) = a^2 + 5b^2 \neq 2$$

for any $a, b \in \mathbb{Z}$.

To show that $(2, 1 + \sqrt{-5}) \neq \mathcal{O}_K$, it is enough to show that $\mathcal{O}_K / 2\mathcal{O}_K$ is a ring over $\mathbb{F}_2$ of dimension 2. Indeed, $\mathcal{O}_K / 2\mathcal{O}_K = \mathbb{F}_2[x]/(x^2 - 1)$, and $1 + \sqrt{-5} \in \mathcal{O}_K$ generates a proper ideal $1 + x$ of $\mathbb{F}_2[x]/(x^2 - 1)$.[2]

There are two problems to deal with. (i) there is no unique decomposition into irreducibles, and (ii) not all ideals are principal.

Lemma 15.1. Let $\mathfrak{a} \subset \mathcal{O}_K$ be a proper ideal. Then $N(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a})$ is finite.

Proof. It is enough to prove for principal ideals that $\mathcal{O}_K \cong \mathbb{Z}^n$; (he then erased the board without elaborating). □

Definition 15.2. We define the Dedekind ζ-function,

$$\zeta_K(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}.$$

If $K = \mathbb{Q}$, this is exactly the Riemann ζ-function.

We want to show that $\zeta_K(s)$ has properites similar to $\zeta_{\mathbb{Q}}(s)$. We also want to discuss its applications, i.e., if m is an integer, then

$$K = K_m = \mathbb{Q}(e^{2\pi i/m}) = \mathbb{Q}(\mu_m),$$

where μ_m is a root of 1 of order m. $\zeta_K(s)$ will be essentially the intersection of $L(\chi, s)$, where $\chi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$. Let R be a ring, and let $\mathfrak{p} \subset R$ be an ideal. We say that $\mathfrak{p}$ is prime if $R/\mathfrak{p}$ has no zero divisors, i.e., for all $\alpha, \beta \in R$ such that $\alpha\beta \in \mathfrak{p}$, either α or β is in $\mathfrak{p}$.

Suppose $\mathfrak{a}_!, \mathfrak{a}_2$ are two ideals of R. Then

$$\mathfrak{a}_1 \cdot \mathfrak{a}_2 = \left\{ \sum_i \alpha_i \beta_i \mid \alpha_i \in \mathfrak{a}_1, \beta_i \in \mathfrak{a}_2 \right\} = \{\alpha\beta \mid \alpha \in \mathfrak{a}_1, \beta \in \mathfrak{a}_2\},$$

which is again an ideal.

Theorem 15.3. For K a number field and $\mathfrak{a} \in \mathcal{O}_K$, there exists a unique decomposition (up to permutation) $\mathfrak{a} = p_1 \dots p_n$ where each p_i is prime.

[2] what are we cooking here

We say that a fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is a finitely generated $\mathcal{O}_K$-submodule of K.

Lemma 15.4. If $\mathfrak{a} \subset \mathcal{O}_K$ is an ideal, then $\mathfrak{a}$ is fractionally generated over $\mathcal{O}_K$ if and only if $\mathcal{O}_K$ is Noetherian.

As an example, consider $K = \mathbb{Q}$ and let $\mathfrak{a} \subset \mathbb{Q}$ be a fractional ideal. Then $\mathfrak{a} = (\alpha)$, where $\alpha \in \mathbb{Q}$; we see that the fractional ideals of $\mathbb{Q}$ are $\mathbb{Q}_{\geq 0}$ with non-zero fractional ideals being isomorphic to $\mathbb{Q}_{>0}$. Under multiplication, $\mathbb{Q}_{>0}$ is an abelian group $\mathbb{Q}^*/\pm 1$. We can define a product of fractional ideals $\mathfrak{a}_1 \cdot \mathfrak{a}_2$, with the product generated by all $\alpha_i \beta_j$.

Theorem 15.5. Nonzero fractional ideals in K form an abelian group with respect to multiplication.

In this way, let F be the group of fractional ideals, and observe that the proper principal fractional ideals are $K^*/\mathcal{O}_K^*$. Let $U(K)$ denote this quotient.

Theorem 15.6. $U(K)$ is finite.

We say that the class number of K is given by $\#U(K)$. If $U(K) = 1$, then all fractional ideals are principal, and so all ideals of $\mathcal{O}_K$ are principal. As an example, consider the quadratic field $\mathbb{Q}(\sqrt{-d})$ where $d > 0$ is square free. We have that the class number is 1 if $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$. It is conjectured that there are infinitely many such d such that the class number of $\mathbb{Q}(\sqrt{d})$ is 1.