Student seminar notes week 5

Erol after the talk of Clerc and Parriaux

Our goal today is to prove Dirichlet's Theorem on Arithmetic progressions, Theorem 4.1 from Childress' book. Let us state the theorem for motivation.

Theorem 0.1. *Let m be a positive integer and a be an integer such that $\gcd(a, m) = 1$. Then, there are infinitely many primes in the sequence $a, m + a, m+2a, \ldots$. In other words, there are infinitely many primes p such that $p \equiv a \mod m$.*

Notice that the special case with $a = 1$ is just the statement that there are infinitely many primes. Let us first give another proof of this fact using the Riemann Zeta function to motivate what is to come. 2000 years after Euclid's proof of the infinitude of primes, Euler gave another proof using what we today call Riemann's Zeta function in 1737. Let us now sketch Euler's proof of the infinitude of primes.
We define the Riemann Zeta function by

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

We will show later in this lecture that the following formula, called Euler's Product Formula, holds:

$$\zeta(s) = \prod_{p} (1 - \frac{1}{p^s})^{-1}$$

This formula is true since we can write every integer as a product of primes using the fundamental theorem of arithmetic. Since in Dedekind domains we can write every ideal as a product of prime ideals, it's natural to expect a generalization to this to Dedekind domains, which we will call the Dedekind Zeta function.
As $s \to 1$, $\zeta(s)$ approaches the harmonic series, which diverges. Thus, the right-handside of the equation above should also diverge. However, if we had finitely many primes, it would not. In fact, in the same paper, Euler shows that $\sum_p \frac{1}{p}$ also diverges and states informally that the sum over all primes of $1/p$ is $\log \log \infty$, which one can see as a primitive version of the Prime Number Theorem!
Let us now start to generalize by defining Dirichlet series.

Definition 0.2. Let $\{a_n\}$ be a sequence of complex numbers. Then,

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

is called a **Dirichlet series**.

Notice that $\zeta(s)$ is a Dirichlet series with the sequence $a_n = 1$ for every $n \geq 1$. Let us now recall some tools we are going to use from complex analysis.

Definition 0.3. Let

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

We say that $f(s)$ **converges pointwise** at $s_0 \in \mathbb{C}$ if

$$S_N(s_0) = \sum_{n=1}^{N} \frac{a_n}{n^s}$$

converges to some $L \in \mathbb{C}$ as $N \to \infty$.
We say that $f(s)$ **converges absolutely** at $s_0 \in \mathbb{C}$ if

$$\sum_{n=1}^{\infty} |\frac{a_n}{n^s}|$$

converges.
We say that $f(s)$ **converges uniformly on** $U \subseteq \mathbb{C}$ if $f(s)$ converges pointwise and

$$\sup_{z \in U} |S_N(z) - f(z)| \to 0$$

as $N \to \infty$.

Let us now recall Abel's Lemma, which follows from a simple trick with telescoping sums and is used in the proof of Abel's Test in real analysis. We omit the proof.

Lemma 0.4. *Let $\{a_n\}, \{b_n\}$ be sequences of complex numbers. Let $r \geq m$. Let $A_{m,r} := \sum_{n=m}^{r} a_n$ and $S_{m,r} := \sum_{n=m}^{r} a_n b_n$.*
Then,

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

Let us also remember the following statement about the convergence of holomorphic functions from complex analysis.

Lemma 0.5. *Let A be an open subset of $\mathbb{C}$ and let $\{f_n\}$ be a sequence of holomorphic functions on A that converge uniformly on every compact subset to f. Then, f is holomorphic on A and $\{f_n'\}$ converges to f' on A.*

The proof is Exercise Sheet 5 Exercise 1.
Finally, here is one last lemma, whose proof is Exercise Sheet 5 Exercise 2:

Lemma 0.6. *If $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges for $s = s_0$, then it converges uniformly in every domain of the form*

$$\{s : Re(s - s_0) \geq 0, |Arg(s - s_0)| \leq \theta\}$$

with $\theta < \frac{\pi}{2}$.

Theorem 0.7. *If $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges for $s = s_0$, then it converges for $Re(s) > Re(s_0)$ to a function that is holomorphic there.*

Let us now sketch the proof.

Proof. Apply Lemma 0.6 and Lemma 0.5 to $A = \{s \in \mathbb{C} : Re(s) > Re(s_0)\}$ and $f_N(s) = \sum_{n=1}^{N} \frac{a_n}{n^s}$. □

Let's now explore some corollaries of this theorem.

Corollary 0.8. *Let*

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

Write $s = \sigma + it$ for $\sigma, t \in \mathbb{R}$.

1. *If the a_n are bounded, then $f(s)$ converges absolutely for $\sigma > 1$.*
2. *If $A_n = a_1 + \cdots + a_n$ is bounded, then $f(s)$ converges (but not necessarily absolutely) for $\sigma > 0$.*
3. *If $f(s)$ converges at $s = s_0$, it converges absolutely for $\sigma > Re(s_0) + 1$.*

Proof. 1. Let $M > 0$ be a real number such that $|a_n| \leq M$ for every $n \geq 0$. Then,

$$\sum_{n=1}^{\infty} |\frac{a_n}{n^s}| \leq \sum_{n=1}^{\infty} \frac{|a_n|}{n^\sigma} \leq M \sum_{n=1}^{\infty} \frac{1}{n^\sigma}.$$

Since the infinite sum on the right-hand side converges for $\sigma > 1$, we have the desired result.

2. For $r \geq m$, let $A_{m,r} := \sum_{n=m}^{r} a_n$ be as in Abel's Lemma.
Let $M > 0$ be a real number such that $|A_{m,r}| \leq M$ for every $r \geq m \geq 0$.
Applying Abel's Lemma with $b_n := n^{-s}$, we get

$$S_{m,r} = \left| \sum_{n=m}^{r-1} A_{m,n}\big(n^{-s} - (n+1)^{-s}\big) + A_{m,r}r^{-s} \right|$$

$$\leq \sum_{n=m}^{r-1} |A_{m,n}|\,|n^{-s} - (n+1)^{-s}| + |A_{m,r}|\,|r^{-s}|$$

$$\leq M\left(\sum_{n=m}^{r-1} |n^{-s} - (n+1)^{-s}| + |r^{-s}| \right).$$

By Theorem 3.2, we can assume without loss of generality that $s = \sigma \in \mathbb{R}$. Then, we have that

$$|S_{m,r}| \leq \frac{M}{m^{\sigma}}$$

, so the partial sums of $f(s)$ are Cauchy when $\sigma > 0$.

3. Let

$$g(s) = f(s + s_0) = \sum_{n=1}^{\infty} \frac{a_n}{n_{s_0}} \frac{1}{n^s}.$$

Since $f(s_0)$ is convergent, $b_n = \frac{a_n}{n^{s_0}} \to 0$ s $n \to \infty$.

Thus, by part (i), $g(s)$ is absolutely convergent for $\sigma > 1$, so $f(s) = g(s - s_0)$ is absolutely convergent when $Re(s - s_0) > 1$.

□

We finally have all of the ingredients ready to generalize the Riemann-Zeta function.

Definition 0.9. Let $\chi : (\mathbb{Z}/m\mathbb{Z})^{\times} \to \mathbb{C}^{\times}$. The **Dirichlet L-series associated to** χ is

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

Notice that $\zeta(s) = L(s, \chi_0)$.
Assume $\chi \neq \chi_0$.
Let $A_n = \chi(1) + \cdots + \chi(n)$. Let $n = mk + r$ where $0 \leq r \leq m - 1$. Then,

$$[\chi(1) + \ldots + \chi(m)] + [\chi(m+1) + \ldots + \chi(2m)] + \cdots$$
$$+ [\chi(km+1) + \ldots + \chi(km+r)]$$
$$= \chi(km+1) + \ldots + \chi(km+r)$$

because $\chi(1)+\ldots+\chi(m) = 0$ by the orthogonality relations. Thus, $A_n \leq r < m$ for any $n \geq 0$.
Thus, by part (ii) of Corollary 3.3, $L(s,\chi)$ is analytic for $Re(s) > 0$. By part (iii), $L(s,\chi)$ converges absolutely for $Re(s) > 1$.
Let us now generalize Euler's product formula. Notice that we also obtain Euler's product formula as a special case when $\chi = \chi_0$.

Proposition 0.10. *Let $s = \sigma + it$ with $\sigma > 1$. Then,*

$$L(s,\chi) = \prod_p (1 - \chi(p)p^{-s})^{-1}.$$

Proof. Fix $s = \sigma + it$ with $\sigma > 1$.
We want to show

$$\lim_{N\to\infty} \prod_{p\leq N} (1 - \frac{\chi(p)}{p^s})^{-1} = L(s,\chi).$$

Let $p_1, \ldots, p_k$ be all the primes less than N.
Then,

$$\prod_{i=1}^{k} (1 - \frac{\chi(p_i)}{p_i^s})^{-1} = \prod_{i=1}^{k} (1 + \frac{\chi(p_i)}{p_i^s} + \frac{\chi(p_i)^2}{p_i^{2s}} + \cdots)$$

since

$$|\frac{\chi(p_i)}{p_i^s}| < 1$$

so we can apply the geometric series formula.
By multiplying the product of sums out, we get

$$\prod_{i=1}^{k} (1 + \frac{\chi(p_i)}{p_i^s} + \frac{\chi(p_i)^2}{p_i^{2s}} + \cdots) = \sum_{m_1,\ldots,m_k\geq 0} \frac{\chi(p_1^{m_1}\cdots p_k^{m_k})}{(p_1^{m_1}\cdots p_k^{m_k})^s}.$$

Let

$$\delta_N = \{n \in \mathbb{Z}_{\geq 0} : n \text{ is not divisible by any prime } p > N\}.$$

Then,

$$\sum_{m_1,\ldots,m_k\geq 0} \frac{\chi(p_1^{m_1}\cdots p_k^{m_k})}{(p_1^{m_1}\cdots p_k^{m_k})^s} = \sum_{n\in\delta_N} \frac{\chi(n)}{n^s}.$$

Thus, we have that

$$L(s,\chi) - \prod_{p\leq N} (1 - \frac{\chi(p)}{p^s})^{-1} = \sum_{n\in\mathbb{Z}_{\geq 0}\setminus\delta_N} \frac{\chi(N)}{n^s}.$$

Taking absolute values and applying the triangle inequality,

$$\sum_{n\in\mathbb{Z}_{\geq 0}\setminus\delta_N} \frac{\chi(N)}{n^s} \leq \sum_{n\in\mathbb{Z}_{\geq 0}\setminus\delta_N} \frac{1}{n^\sigma}.$$

As $N \to \infty$, the right hand-side goes to zero for $\sigma > 1$. □

If $Re(s) > 1$, we have that $L(s,\chi) \neq 0$. This is because we showed in Lecture 4 that $\log L(s,\chi)$ is convergent for $Re(s) > 1$, and this implies that the infinite product can't diverge. It also can't converge to zero since otherwise the logarithm would have to diverge to negative infinity. (In general, infinite products are said to converge if the product converges to a non-zero number. If the product converges to zero, the product is said to diverge to zero.)
Let log be the principal branch of the logarithm, so the argument is between $-\pi$ and π.
Taking logarithm and using the Taylor series for $\log(1-t)$, we obtain

$$\log(L(s,\chi)) = -\sum_p \log(1-\chi(p)p^{-s}) = \sum_p \sum_{n\geq 1} \frac{\chi(p)^n}{np^{ns}}.$$

Now, notice that

$$\sum_p \sum_{n\geq 1} |\frac{\chi(p)^n}{np^{ns}}| \leq \sum_p \sum_{n\geq 1} \frac{1}{p^{n\sigma}} \leq \sum_{m\geq 1} \frac{1}{m^\sigma}.$$

The last inequality holds because instead of summing over all the numbers of the form p^n, we are summing over all natural numbers, so we are adding positive terms to the series, which can only make it larger.
Thus, $\log(L(s,\chi))$ converges absolutely for $\sigma > 1$ so we can rearrange terms to get

$$\log(L(s,\chi)) = \sum_p \frac{\chi(p)}{p^s} + \sum_p \sum_{n\geq 2} \frac{\chi(p)^n}{np^{ns}}.$$

Let

$$\beta(s,\chi) = \sum_p \sum_{n\geq 2} \frac{\chi(p)^n}{np^{ns}}.$$

Notice that

$$|\sum_{n\geq 2} \frac{\chi(p)^n}{np^{ns}}| \leq \sum_{n\geq 2} \frac{1}{p^{n\sigma}} = \frac{p^{-2\sigma}}{1-p^{-\sigma}}.$$

Thus,

$$|\sum_p \sum_{n\geq 2} \frac{\chi(p)^n}{np^{ns}}| \leq \sum_p \frac{p^{-2\sigma}}{1-p^{-\sigma}}.$$

Since there are finitely many primes with $p^{-\sigma} \geq \frac{1}{2}$, we can ignore them completely and so we can ignore the denominator for the remaining infinitely many primes. Thus, this is essentially

$$\sum_p p^{-2\sigma}$$

which converges absolutely for $\sigma > 1/2$.
We are now ready to prove Dirichlet's Theorem on Primes in Arithmetic Progressions, Theorem 0.1, which was stated in the beginning of the lecture.
Before diving into the proof, let us state some definitions and results we will use.

Definition 0.11. Let K be an algebraic number field. We define the **Dedekind zeta function of** K to be

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N\mathfrak{a}^s}$$

, as $\mathfrak{a}$ runs over all non-zero integral ideals of $\mathcal{O}_K$.

It is Exercise 3 on Sheet 5 to prove that $\zeta_K(s)$ is absolutely convergent for $\mathrm{Re}(s) > 1$.
By using factorizations of ideals instead of numbers, we have that

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s})^{-1}$$

as $\mathfrak{p}$ runs over the prime ideals of $\mathcal{O}_K$. Let

$$\gamma_n = \{\mathfrak{a} : N\mathfrak{a} = n\}.$$

Then,

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

We leave it as an exercise to show that $\zeta_K(s)$ is absolutely convergent for $Re(s) > 1$.
We will also use the following theorem without proof.

Theorem 0.12. *$\zeta_K(s)$ can be analytically continued to $\mathbb{C} - \{1\}$, with a simple pole at $s = 1$, i.e.*

$$\zeta_K(s) = \frac{\rho(K)}{s-1} + \textit{(something entire).}$$

Moreover,

$$\rho(K) = \frac{2^{r_1}(2\pi)^{r_2} h_K r_K}{w_K \sqrt{|d_{K/\mathbb{Q}}|}}$$

where r_1 is the number of real embeddings of K, r_2 is the number of pairs of conjugate complex embeddings of K, h_K is the class number of K, R_K is the regulator of K, w_K is the number of roots of unity in K and $d_{K/\mathbb{Q}}$ is the discriminant.

We will also use the following lemma whose proof is Sheet 5 Exercise 4:

Lemma 0.13. *Let p, m be natural numbers with p prime such that $p \nmid m$. Let f be the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$. Then,*

$$(1 - T^f)^{\varphi(m)/f} = \prod_{\chi \mod m} (1 - \chi(p)T)$$

where T is a variable.

We can now begin the proof.

Proof. Let $\gcd(m, a) = 1$. Notice that as the sums run over all characters of $(\mathbb{Z}/m\mathbb{Z})^\times$,

$$\begin{aligned}\sum_\chi \chi(a)^{-1} \log L(s, \chi) &= \sum_\chi \chi(a)^{-1} \left(\sum_p \frac{\chi(p)}{p^s} + \beta(s, \chi) \right) \\ &= \sum_p \frac{1}{p^s} \sum_\chi \chi(a)^{-1}\chi(p) + \sum_\chi \chi(a)^{-1}\beta(s, \chi) \\ &= \sum_p \frac{1}{p^s} \sum_\chi \chi(pa^{-1}) + \sum_\chi \chi(a)^{-1}\beta(s, \chi).\end{aligned}$$

But, by the orthogonality relations,

$$\sum_\chi \chi(pa^{-1}) = \begin{cases} \varphi(m), & p \equiv a \pmod m, \\ 0, & \text{otherwise,} \end{cases}$$

so

$$\sum_\chi \chi(a)^{-1} \log L(s, \chi) = \varphi(m) \sum_{p \equiv a \pmod m} p^{-s} + G(s), \qquad (*)$$

where $G(s)$ is just some series which is absolutely convergent for $\Re(s) > \frac{1}{2}$.
Let $s \to 1$. For the right-hand side of (*)
we get

$$\lim_{s \to 1} \varphi(m) \sum_{p \equiv a \mod m} p^{-s} + \text{some finite constant}$$

which would be finite if there were finitely many primes with $p \equiv a \mod m$. Thus, the proof will be complete if we can show that the left-hand side is infinite. We already know that if $\chi = \chi_0$ we have

$$L(s,\chi_0) = \prod_p (1-\chi_0(p)p^{-s})^{-1} = \zeta(s)\prod_{p|m}(1-p^{-s}) \to \infty$$

as $s \to 1$ so $\log L(s,\chi_0) \to \infty$ as $s \to 1$.
Thus, it suffices to show that the non-trivial characters don't cancel this out. Recall that by the orthogonality relations, the sums over the characters are bounded. Thus, by Corollary 3.3 part (ii), $L(s,\chi)$ is analytic for $Re(s) > 0$. Thus, we only need to show that $L(1,\chi) \neq 0$.
Let $K = \mathbb{Q}(\zeta_m)$. Thus,

$$\begin{aligned}
\zeta_K(s) &= \prod_{\mathfrak{p}} \left(1 - N\mathfrak{p}^{-s}\right)^{-1} \\
&= \prod_p \prod_{\mathfrak{p}|p} \left(1 - N\mathfrak{p}^{-s}\right)^{-1} \\
&= \left(\prod_{p|m} \prod_{\mathfrak{p}|p} \left(1 - N\mathfrak{p}^{-s}\right)^{-1}\right) \left(\prod_{p\nmid m} \prod_{\mathfrak{p}|p} \left(1 - N\mathfrak{p}^{-s}\right)^{-1}\right).
\end{aligned}$$

Notice that $N\mathfrak{p} = p^f$ where f is residue field degree.
Now, by Lemma 0.13, we have that

$$\prod_{p\nmid m}(1-p^{-sf})^{-\varphi(m)/f} = \prod_{\chi}\prod_{p\nmid m}(1-\chi(p)p^{-s})^{-1}.$$

Now, if $p \mid m$, then $\chi(p) = 0$, so they don't contribute, and we have

$$\begin{aligned}
\prod_{p\nmid m}(1-p^{-sf})^{-\varphi(m)/f} &= \prod_p (1-p^{-sf})^{-\varphi(m)/f} \\
&= \prod_p \prod_{\chi} (1-\chi(p)p^{-s})^{-1} \\
&= \prod_{\chi} \prod_p (1-\chi(p)p^{-s})^{-1} \\
&= \prod_{\chi} L(s,\chi).
\end{aligned}$$

On the other hand,

$$\prod_{p\nmid m}(1-p^{-sf})^{-\varphi(m)/f} = \prod_{p\nmid m}\prod_{\mathfrak{p}|p}(1-N\mathfrak{p}^{-s})^{-1} = \zeta_K(s)\prod_{p|m}\prod_{\mathfrak{p}|p}(1-N\mathfrak{p}^{-s})^{-1}.$$

Thus,

$$\begin{aligned}
&\zeta_K(s) \prod_{p|m} \prod_{\mathfrak{p}|p} (1 - N\mathfrak{p}^{-s})^{-1} \\
&\quad = \prod_{\chi} L(s, \chi) \\
&\quad = L(s, \chi_0) \prod_{\chi \neq \chi_0} L(s, \chi) \\
&\quad = \zeta(s) \prod_{p|m} (1 - p^s) \prod_{\chi \neq \chi_0} L(s, \chi).
\end{aligned}$$

Finally, we have

$$\frac{\left(\prod_{p|m} \prod_{p|\mathfrak{p}} (1 - N\mathfrak{p}^{-s})\right) \zeta_K(s)}{\left(\prod_{p|m} (1 - p^{-s})\right) \zeta(s)} = \prod_{\chi \neq \chi_0} L(s, \chi).$$

Notice that both products over $p \mid m$ are non-zero constants. Since both ζ and ζ_K have a simple pole at $s = 1$, we can let $s \to 1$ and the expression on the left approaches a finite constant, so the right-handside does too. We thus conclude the proof. $\square$