Week 6 Summary

Declan Fletcher

Abstract

We summarise section 1 and 2 of chapter 8 of SS. The goal of the chapter is to prove *Dirichlet's theorem on primes in arithmetic progressions*. Section 1 provides motivation for the proof by presenting an earlier analytic-flavoured proof in number theory, then section 2 sketches the proof of Dirichlet's theorem.

The goal of chapter 8 of SS is to prove *Dirichlet's theorem*:

Theorem 1 (Dirichlet's theorem on primes in arithmetic progressions)**.** *Let l and q be coprime positive integers. Then the arithmetic progression*

$$l,\, l+q,\, l+2q,\, l+3q,\, \ldots,\, l+kq,\, \ldots$$

contains infinitely many prime numbers.

This striking result refines the classical fact that there are infinitely many primes, by informing us that if l and q are coprime positive integers, there are in particular infinitely many primes congruent to l modulo q. As a concrete example, for $l = 1$ and $q = 4$, the theorem says that there are infinitely many primes in the arithmetic progression

$$1,\, 5,\, 9,\, 13,\, 17,\, 21,\, \ldots$$

The proof of the theorem utilises the theory of Fourier analysis on the finite abelian group $\mathbb{Z}^*(q)$, and indicates the power that Fourier analysis and analysis generally have to prove results in number theory.

Number Theory and Analysis

Before discussing the proof of Dirichlet's theorem, we need to understand an earlier result which informed Dirichlet's theorem, since it is not clear a priori how analysis would be used to prove theorems in number theory.

Euler was one of first mathematicians who linked the worlds of number theory and analysis. He studied the zeta function, which is defined for a real number $s > 1$ by

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

(Note that ζ has an analytic continuation to a meromorphic function on the complex plane, but for now we have just defined $\zeta(s)$ for real $s > 1$.) The zeta function is an

object in the world of analysis, but *Euler's product formula* relates the zeta function to the primes and the world of number theory:

Theorem 2 (Euler's product formula)**.** *For real $s > 1$, we have that*

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

where the product is over all prime numbers p.

The Euler product is an analytic expression of the fundamental theorem of arithmetic. An interesting fact that SS prove as a consequence of the Euler product formula is the following:

Theorem 3. *The series*

$$\sum_p \frac{1}{p},$$

where the sum is taken over all primes p, diverges.

Since the series would converge if there were only finitely many primes, this result gives a new (analytic!) proof of the fact that there are infinitely many primes. This is Euler's proof of the infinitude of the primes.

Dirichlet's Theorem

Dirichlet realised that he could use the idea of Euler's proof to prove Theorem 1. In particular, he realised that to show that the arithmetic progression

$$l,\, l+q,\, l+2q,\, l+3q,\, \ldots,\, l+kq,\, \ldots$$

contains infinitely many primes, it is sufficient to show that the series

$$\sum_{p \equiv l \bmod q} \frac{1}{p}$$

diverges. Specifically, the proof of the theorem shows that

$$\sum_{p \equiv l \bmod q} \frac{1}{p^s}$$

diverges as $s \to 1^+$. The details of the proof are subtle, but we now introduce some key ideas used.

Let q and l be coprime positive integers and let G be the finite abelian group $\mathbb{Z}^*(q)$. For the proof of Dirichlet's theorem, we extend certain functions on G to functions on all of $\mathbb{Z}$. For an example of this, consider the indicator function of $l \in G$ as a function on G,

$$\delta_l(n) = \begin{cases} 1 & \text{if } n \equiv l \mod q, \\ 0 & \text{otherwise.} \end{cases}$$

To extend δ_l to a function on $\mathbb{Z}$, we set $\delta_l(m) = 0$ if m and q are not relatively prime. In a similar way, we can extend characters of G to functions on $\mathbb{Z}$. If $e \in \hat{G}$, we define

$$\chi(m) = \begin{cases} e(m) & \text{if } m \text{ and } q \text{ are relatively prime,} \\ 0 & \text{otherwise.} \end{cases}$$

The function χ is called a *Dirichlet character* modulo q. The notation χ_0 is used for the extension of the trivial character, i.e., $\chi_0(m) = 1$ if m and q are relatively prime and $\chi_0(m) = 0$ otherwise. Fourier analysis on G can be used to prove the following result:

Lemma 4. *The Dirichlet characters are multiplicative. Moreover,*

$$\delta_l(m) = \frac{1}{\varphi(q)} \sum_{\chi} \overline{\chi(l)}\chi(m),$$

where the sum is over all Dirichlet characters.

Here $\varphi(q)$ is Euler's totient function, which counts the number of positive integers less than or equal to q which are coprime to q, which is also the order of the group G. Note that δ_l is the indicator function of the arithmetic series l, $l + q$, $l + 2q$, ... Then Lemma 4 allows us to rewrite the series we are interested in in the following way:

$$\sum_{p \equiv l \bmod q} \frac{1}{p^s} = \sum_{p} \frac{\delta_l(p)}{p^s} = \frac{1}{\varphi(q)} \sum_{p} \sum_{\chi} \overline{\chi(l)} \frac{\chi(p)}{p^s}. \tag{1}$$

Through some careful analytic manipulation of the right hand side of equation 1, we can show the left hand series diverges as $s \to 1^+$.

When making the necessary analytic manipulations, we are led to consider so-called *Dirichlet L-functions*. These are defined for real $s > 1$ by

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

where χ is a Dirichlet character. For example, let e be the character of $\mathbb{Z}^*(4)$ defined by $e(1) = 1$ and $e(3) = -1$. Then the corresponding Dirichlet character χ is given by $\chi(n) = 1$ if $n \equiv 1 \mod 4$, $\chi(n) = -1$ if $n \equiv 3 \mod 4$ and $\chi(n) = 0$ if n is even. Thus,

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} - \frac{1}{11^s} + \dots$$

Dirichlet proved L-functions can be expressed as products analogous to the Euler product.

Theorem 5. *If $s > 1$, then*

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

where the product is over all primes p.

This expression for $L(s, \chi)$ plays an important role in showing that the series in equation 1 diverges as $s \to 1^+$.