

Chapter 7

Primes in Arithmetic Progression

7.1 Introduction

In Chapter 1, we have seen Euclid's proof of the existence of infinitely many primes. His proof can be extended to prove that there are infinitely many primes of the form $4n + 3$ and $6n + 5$. However his method fails if one wants to prove that there are infinitely many primes of the form $4n + 1$, and in general the infinitude of primes of the form $an + b$, with $(a, b) = 1$.

In this Chapter we shall prove Dirichlet's Theorem :

Theorem 7.1.1 *If $(k, l) = 1$ then*

$$\sum_{\substack{p \leq x \\ p \equiv l \pmod{k}}} \frac{1}{p} = \frac{\log \log x}{\varphi(k)} + O(1).$$

The above theorem immediately implies that there are infinitely many primes of the form $kn + l$. Note that this is indeed the analogue of the Merten estimates.

7.2 Dirichlet Characters

Definition. A Dirichlet character $(\bmod k)$ is an arithmetic function

$$\chi : \mathbb{N} \rightarrow \mathbb{C}$$

satisfying

- (i) $\chi(mn) = \chi(m)\chi(n)$ for all $m, n \in \mathbb{N}$.
- (ii) $|\chi(n)| = \begin{cases} 1 & \text{if } (n, k) = 1 \\ 0 & \text{otherwise.} \end{cases}$
- (iii) $\chi(n + km) = \chi(n)$ for all $n, m \in \mathbb{N}$,
- (iv) $\chi^{\varphi(k)}(n) = 1, (n, k) = 1$.

Here are some elementary properties of χ .

- (i) Values of χ are 0 or $\varphi(k)^{th}$ roots of unity.
- (ii) There are only finitely many characters $(\text{mod } k)$, namely, $\leq \varphi(k)^{\varphi(k)}$.
- (iii) If χ_1 and χ_2 are characters $(\text{mod } k)$, then so is $\chi_1\chi_2$.
- (iv) A character $\chi(\text{mod } k)$ can be regarded as homomorphism

$$\chi : G_k \rightarrow \{z \in \mathbb{C} \mid |z| = 1\}$$

where G_k is the group of residue classes $(\text{mod } k)$, $(n, k) = 1$ with multiplication as group operation.

Theorem 7.2.1 *There are exactly $\varphi(k)$ characters $(\text{mod } k)$.*

Proof. From the structure theorem of abelian group, we know that G_k can be written as a direct sums of cyclic group with prime power order say

$$G_k = \mathbb{Z}_{h_1} \oplus \cdots \oplus \mathbb{Z}_{h_r}$$

where h_i are prime powers. Let $a \in G_k$. Then $a = a_1^{\alpha_1} \cdots a_r^{\alpha_r}$ where $0 \leq \alpha_i \leq h_i - 1$ and a_i 's are generators for \mathbb{Z}_{h_i} . Now

$$\chi(a) = \prod_i \chi(a_i)^{\alpha_i}.$$

Each χ depends on its value on a_i , and since there are at most $\varphi(k)$ elements in G_k , there are at most $\varphi(k)$ of such χ .

Next, given w_1, \dots, w_r such that

$$w_i^{h_i} = 1,$$

for all i . By setting $\chi(a_i) = w_i$ and defining $\chi(n)$ by

$$\chi(n) = \begin{cases} \prod_i \chi(a_i)^{\alpha_i} & \text{if } (n, k) = 1 \\ 0 & \text{otherwise,} \end{cases}$$

we can show that χ is a character. Hence, we have at least $h_1 \cdots h_r = \varphi(k)$ characters. This shows that there are exactly $\varphi(k)$ characters (mod k).

The character χ_0 will always denote the principal character (mod k), i.e.,

$$\chi_0(n) = \begin{cases} 1 & \text{if } (n, k) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

The character $\bar{\chi}$ will denote the inverse of χ , or, $\chi \cdot \bar{\chi} = \chi_0$.

Remarks. The above Theorem is a special case from a more general Theorem in the theory of characters. In general a linear representation is a homomorphism $\rho : G \rightarrow GL_n(F)$, where F is a field. A character is defined to be $\chi(g) = \text{Trace}(\rho(g))$. In general, χ is not a homomorphism. However, when G is abelian, all irreducible representations are 1-dimensional over F . In this case, $\chi(g) = \rho(g)$, and so, χ is a homomorphism. Furthermore, from character theory, we know that there are exactly C irreducible characters for a finite group with C conjugacy classes. When G is abelian, each element represents a single conjugacy class and so, there are exactly $|G|$ conjugacy classes, hence exactly $|G|$ characters. This explains why there are exactly $\varphi(k)$ characters (mod k).

7.3 Orthogonal relations

Theorem 7.3.1 (i) Let χ_1, χ_2 be 2 characters (mod k). Then

$$\sum_{a=1}^k \chi_1(a) \overline{\chi_2(a)} = \begin{cases} \varphi(k) & \text{if } \chi_1 = \chi_2 \\ 0 & \text{otherwise,} \end{cases}$$

(ii) Let a_1, a_2 be integers with $(a_i, k) = 1$. Then

$$\sum_{\chi \pmod k} \chi(a_1) \overline{\chi(a_2)} = \begin{cases} \varphi(k) & \text{if } a_1 = a_2 \\ 0 & \text{otherwise,} \end{cases}$$

This theorem is another special case of character theory. They are known as the first and second orthogonality relations for characters.

Proof of (i). Set $\chi = \chi_1 \overline{\chi_2}$. Then the relation becomes,

$$\sum_{a=1}^k \chi(a) = \begin{cases} \varphi(k) & \text{if } \chi = \chi_0 \\ 0 & \text{otherwise.} \end{cases}$$

If $\chi = \chi_0$ then

$$\sum_{a=1}^n \chi(a) = \varphi(k).$$

If $\chi \neq \chi_0$, then there exist an a_0 coprime to k such that $\chi(a_0) \neq 1$. Now,

$$\chi(a_0) \sum_{a=1}^k \chi(a) = \sum_a \chi(a_0 a) = \sum_a \chi(a).$$

Therefore, $\sum_a \chi(a) = 0$.

Proof of (ii). Let $a = a_1 \overline{a_2}$, where $\overline{a_2}$ = inverse of $a_2 \pmod k$. Then

$$\chi(a_1) \overline{\chi(a_2)} = \chi(a_1) \chi(\overline{a_2}) = \chi(a_1 \overline{a_2}) = \chi(a).$$

So, (ii) becomes

$$\sum_{\chi \pmod k} \chi(a) = \begin{cases} \varphi(k) & \text{if } a \equiv 1 \pmod k \\ 0 & \text{otherwise,} \end{cases}$$

First case is trivial. Second case : There exist χ^* so that $\chi^*(a) \neq 1$. So,

$$\chi^*(a) \sum_{\chi} \chi(a) = \sum_{\chi} \chi^* \chi(a) = \sum_{\chi} \chi(a).$$

Hence the result.

7.4 Dirichlet L -series

Definition. The Dirichlet L -series is defined as

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

Theorem 7.4.1

- (i) If $\chi = \chi_0$ then $L(s, \chi)$ can be analytically continued to the half-plane $\sigma > 0$, with the exception of the point $s = 1$ where it has a simple pole with residue $\varphi(k)/k$.
- (ii) If χ is not the principal character (mod k), then $L(s, \chi)$ can be analytically continued to $\sigma > 0$.

Proof. For $\sigma > 1$, we have by Euler's Product Formula,

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

$$L(s, \chi_0) = \prod_{p \nmid k} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{p|k} \left(1 - \frac{1}{p^s}\right).$$

The function $\zeta(s)$ has analytic continuation with residue 1 at $s = 1$. So the residue of $L(s, \chi_0)$ is $\varphi(k)/k$.

Proof of (ii). If $\chi \neq \chi_0$, then $\sum_{n=1}^k \chi(n) = 0$. so,

$$\left| \sum_{n \leq x} \chi(n) \right| \leq k,$$

for $n \geq 1$. Hence

$$\left| \sum_{y \leq n \leq x} \frac{\chi(n)}{n^s} \right| \leq \frac{1}{|y^s|} \sum_{y \leq n \leq x} \chi(n) \rightarrow 0$$

as $y \rightarrow \infty$. This implies that the L -series converges for $\sigma > 0$, and hence, represents an analytic continuation to $\sigma > 0$.

7.5 Proof of Dirichlet Theorem

Step 1. It is enough to show that

$$\sum_{\substack{p \\ p \equiv l \pmod{k}}} \frac{1}{p^\sigma} = \frac{1}{\varphi(k)} \log \frac{1}{\sigma - 1} + O(1),$$

as $\sigma \rightarrow 1+$.

Let

$$\Sigma_1 = \sum_{p \equiv l \pmod{k}} \frac{1}{p^\sigma},$$

and

$$\Sigma_2 = \sum_{\substack{p \leq x \\ p \equiv l \pmod{k}}} \frac{1}{p},$$

and set $\sigma = 1 + \frac{1}{\log x}$.

$$|\Sigma_1 - \Sigma_2| \leq \underbrace{\sum_{p \leq x} \left(\frac{1}{p} - \frac{1}{p^\sigma} \right)}_{\Sigma_3} + \underbrace{\sum_{p > x} \frac{1}{p^\sigma}}_{\Sigma_4}$$

$$\begin{aligned} \Sigma_3 &= \sum_{p \leq x} \frac{1 - e^{-(\sigma-1) \log p}}{p} \leq \sum_{p \leq x} \frac{(\sigma-1) \log p}{p} \\ &= \frac{1}{\log x} \sum_{p \leq x} \frac{\log p}{p} = O(1). \end{aligned}$$

$$\begin{aligned}
\Sigma_4 &= \lim_{y \rightarrow \infty} \sum_{x \leq p \leq y} \frac{1}{p^\sigma} \\
&= \lim_{y \rightarrow \infty} \left(\frac{1}{y^\sigma} \sum_{p \leq y} 1 - \frac{1}{x^\sigma} \sum_{p \leq x} 1 - \int_x^y \sum_{p \leq t} 1 \left(-\frac{\sigma}{t^{\sigma+1}} \right) dt \right) \\
&= O(1) + \int_x^\infty O\left(\frac{t}{\log t}\right) \frac{dt}{t^{\sigma+1}} \\
&= O(1) + O\left(\int_x^\infty \frac{dt}{t^\sigma \log t}\right) \\
&= O(1) + O\left(\frac{1}{\log x} \int_x^\infty \frac{dt}{t^\sigma}\right) = O(1).
\end{aligned}$$

Therefore, if

$$\sum_{\substack{p \leq x \\ p \equiv l \pmod{k}}} \frac{1}{p^\sigma} = \frac{1}{\varphi(k)} \log \frac{1}{\sigma - 1} + O(1), \sigma = 1 + \frac{1}{\log x},$$

then Dirichlet's Theorem holds.

Step 2.

$$\begin{aligned}
\sum_{p \equiv l \pmod{k}} \frac{1}{p^\sigma} &= \sum_p \frac{1}{p^\sigma} \left(\frac{1}{\varphi(k)} \sum_{\chi \pmod{k}} \overline{\chi(l)} \chi(p) \right) \\
&= \frac{1}{\varphi(k)} \sum_{\chi \pmod{k}} \overline{\chi(l)} S(\sigma, \chi),
\end{aligned}$$

where

$$S(\sigma, \chi) = \sum_p \frac{\chi(p)}{p^\sigma}.$$

Now,

$$\sum_p \sum_{m \geq 1} \frac{1}{mp^{m\sigma}} - \sum_p \frac{1}{p^\sigma} = -\log \left(1 - \frac{1}{p^\sigma} \right) - \sum_p \frac{1}{p^\sigma} = O(1),$$

since

$$\sum_p \sum_{m \geq 2} \frac{1}{mp^{m\sigma}} \leq \frac{1}{2} \sum_p \sum_{m \geq 2} \frac{1}{p^{m\sigma}} = \frac{1}{2} \sum_p \frac{1}{p^\sigma(p^\sigma - 1)} = O(1).$$

Therefore,

$$\begin{aligned}
 S(\sigma, \chi_0) &= \sum_p \sum_{m \geq 1} \frac{1}{mp^{m\sigma}} + O(1) \\
 &= - \sum_p \log \left(1 - \frac{1}{p^\sigma} \right) + O(1) \\
 &= \log \prod_p \left(1 - \frac{1}{p^\sigma} \right) + O(1) \\
 &= \log \zeta(\sigma) + O(1) \\
 &= \log \left(\frac{1}{\sigma - 1} \right) + O(1) \\
 &= \log \frac{1}{\sigma - 1} + O(1),
 \end{aligned}$$

for $1 < \sigma \leq \sigma_0, \sigma_0 > 1$. So, we see that the main term comes from the principal character χ_0 . Hence, it remains to show that

$$S(\sigma, \chi) = O(1)$$

for $1 < \sigma \leq \sigma_0$ and all non-principal character $\chi \pmod{k}$.

Step 3.

$$\begin{aligned}
 S(\sigma, \chi) &= \sum_p \frac{\chi(p)}{p^\sigma} = \sum_p \sum_{m \geq 1} \frac{\chi(p)^m}{mp^{m\sigma}} + O(1) \\
 &= - \sum_p \log \left(1 - \frac{\chi(p)}{p^\sigma} \right)^{-1} + O(1) \\
 &= \log(L(\sigma, \chi)) + O(1).
 \end{aligned}$$

Now, for $\chi \neq \chi_0$ $L(s, \chi)$ is analytic in $\sigma > 0$. So, $L(\sigma, \chi)$ is continuous and therefore $\lim_{\sigma \rightarrow 1} L(\sigma, \chi)$ exists and is $L(1, \chi)$. If $L(1, \chi) \neq 0$ then we are done. So, it remains to show that $L(1, \chi) \neq 0$.

Step 4. $L(1, \chi) \neq 0$ for $\chi \neq \chi_0$ and χ is a complex character. Consider

$$P(\sigma) = \prod_{\chi \pmod{k}} L(\sigma, \chi)$$

which gives

$$\begin{aligned}
 \log P(\sigma) &= \sum_{\chi(\bmod k)} \log L(\sigma, \chi) \\
 &= \sum_{\chi(\bmod k)} \sum_p \sum_{m \geq 1} \frac{\chi(p^m)}{mp^{m\sigma}} \\
 &= \sum_p \sum_{m \geq 1} \frac{1}{mp^{m\sigma}} \sum_{\chi(\bmod k)} \chi(p^m) \overline{\chi(1)} \\
 &= \sum_p \sum_{\substack{m \geq 1 \\ p^m \equiv 1(\bmod k)}} \frac{1}{mp^{m\sigma}} \geq 0
 \end{aligned}$$

for $\sigma > 1$. Hence, $P(\sigma) \geq 1$ for $\sigma > 1$. Now suppose $L(1, \chi) = 0$ for some χ . Then $L(1, \bar{\chi}) = 0$. Hence, $P(s)$ has two zeros at $s = 1$. But $L(s, \chi_0)$ has a simple pole at $s = 1$, which means that $P(1) = 0$. This is a contradiction.

Step 5. $L(1, \chi) \neq 0$ for real characters χ . Consider the function $f = \chi * 1$, f is multiplicative. At prime power,

$$\sum_{l=0}^m \chi(p^l) = \begin{cases} 1 & \text{if } p|k \\ \geq 1 & \text{if } p \nmid k, m \text{ even} \\ \geq 0 & \text{if } p \nmid k, m \text{ odd} \end{cases}$$

Thus, $f(n) \geq 0$ for all n and ≥ 1 when n is a square. Hence,

$$F(\sigma) = \sum_{n \geq 1} \frac{f(n)}{n^\sigma} \geq \sum_{m \geq 1} \frac{1}{m^{2\sigma}} = \zeta(2\sigma).$$

In particular, $F(\sigma)$ diverges at $\sigma = 1/2$ and so $\sigma_c \geq 1/2$. By Landau's Theorem in the previous chapter, $F(s)$ must have a singularity at $s = \sigma_c \geq 1/2$. For $\sigma > 1$,

$$F(s) = L(s, \chi)\zeta(s).$$

If $L(1, \chi) = 0$, then $F(s)$ would be analytic in $\sigma > 0$, and thus would not have a singularity at $\sigma_c \geq 1/2$.

Remark. Dirichlet's Theorem is a special case of the Chebotarev Density Theorem.