Chapter 8

Primes in arithmetic progressions

8.1 Characters of finite abelian groups

Definition 8.1 (Character)**.** *Let G be a finte abelian group. A **character** of G is a homomorphism of G into the multiplicative group $\mathbb{C}^\times$ of non-zero complex numbers.*

Remark. Let G be a finite abelian group of order n. Let χ be a character of G. Then for any $g \in G$, we have

$$\chi(g)^n = \chi(g^n) = \chi(1) = 1.$$

In particular, we have $|\chi(g)| = 1$. So a character actually maps G into the unit circle.

Let χ_1, χ_2 be characters of G. Then $\chi_1\chi_2$ and χ_1^{-1} are also characters of G. Therefore, the characters of G forms an abelian group.

Definition 8.2 (Dual group)**.** *We denote by $\widehat{G}$ the group of characters of G. It is called the **dual group** of G.*

Example 8.1. *Let G be a cyclic group of order n with generator g. We study the structure of G. Clearly, any character $\chi \in \widehat{G}$ is determined by its value at g and $\chi(g)$ must be an n-th root of unity. Conversely, given an n-th root of unity w, the map*

$$g^k \mapsto w^k$$

defines a character of G. So $\widehat{G} \cong \mathbb{Z}/n\mathbb{Z} \cong G$.

Lemma 8.1. *Let H be a subgroup of a finite abelian group G. Every character of H extend to a character of G.*

Proof. We prove by induction on the index $(G : H)$. If $(G : H) = 1$, there is nothing to prove. Otherwise we can take some $g \in G$ with $g \notin H$. Let H' be the subgroup of G generated by H and g. Then every $h' \in H'$ can be written as $h' = g^k h$ with some $k \in \mathbb{Z}$ and some $h \in H$.

Now given a character χ of H, we want to extend χ to H'. Let n be the smallest integer > 1 such that $g^n \in H$. Choose $w \in \mathbb{C}^\times$ such that $w^n = \chi(g^n)$. This is possible since $\mathbb{C}$ is algebraically closed. We consider the map

$$\begin{aligned} \chi' : H' &\to \mathbb{C}^\times \\ g^k h &\mapsto w^k \chi(h). \end{aligned}$$

We claim that χ' is a character of H' extending χ. Since it is clear that χ' is a homomorphism and $\chi'|_H = \chi$, it suffices to show χ' is well-defined. In fact, suppose that

$$g^{k_1} h_1 = g^{k_2} h_2, \qquad k_1, k_2 \in \mathbb{Z}, \quad h_1, h_2 \in H.$$

Then we have $g^{k_1 - k_2} = h_2 h_1^{-1} \in H$. By the minimality of n, it follows that $k_1 = k_2 + ln$ for some $l \in \mathbb{Z}$. So we have

$$g^{k_2 + ln} h_1 = g^{k_1} h_1 = g^{k_2} h_2 \quad \Rightarrow \quad g^{ln} h_1 = h_2.$$

Hence

$$w^{k_1} \chi(h_1) = w^{k_2 + ln} \chi(h_1) = w^{k_2} \chi(g^{ln} h_2) = w^{k_2} \chi(h_2).$$

This implies that χ' is well-defined. Therefore, we have extended χ to H'. Since $(G : H') < (G : H)$, we can further extend this character to G by the inductive hypothesis. □

Remark. Let $f : G_1 \to G_2$ be a homomorphism of abelian groups. Then f induces a homomorphism $\widehat{f} : \widehat{G}_2 \to \widehat{G}_1$ defined by

$$\widehat{f}(\chi)(g) = \chi(f(g)), \quad g \in G_1, \, \chi \in \widehat{G}_2.$$

Let H be a subgroup of G. Then we have two natrual morphisms:

$$\rho_1 : H \hookrightarrow G, \qquad \rho_2 : G \to G/H.$$

They induce the following morphisms:

$$\widehat{\rho}_1 : \widehat{G} \to \widehat{H}, \qquad \widehat{\rho}_2 : \widehat{G/H} \to \widehat{G}.$$

Lemma 8.1 tells us $\widehat{\rho}_1$ is surjective and obviously $\widehat{\rho}_2$ is injective. The kernel of $\widehat{\rho}_1$ is the set of characters of G which acts trivially on H, hence is equal to the image of $\widehat{\rho}_2$. Therefore, we have the following exact sequence:

$$1 \to \widehat{G/H} \to \widehat{G} \to \widehat{H} \to 1.$$

In particular, we have $|\widehat{G}| = |\widehat{H}| \cdot |\widehat{G/H}|$.

Theorem 8.2. *The group $\widehat{G}$ is a finite abelian group of the same order with G.*

Proof. We prove by induction on the order n of G. If $n = 1$, the conclusion is trivial. If $n \geq 2$, we choose a non-trivial cyclic subgroup H of G. Then we have $|H| = |\widehat{H}|$ since H is cyclic (see Example 8.1) and $|G/H| = |\widehat{G/H}|$ by the inductive hypothesis. By the above remark, we have

$$|G| = |G/H| \cdot |H| = |\widehat{G/H}| \cdot |\widehat{H}| = |\widehat{G}|.$$

The proof is complete. □

Every $g \in G$ can be viewed as a character of $\widehat{G}$ by

$$g : \chi \mapsto \chi(g).$$

Thus we obtain a homomorphism $\varepsilon : G \to \widehat{\widehat{G}}$.

Theorem 8.3. *The homomorphism $\varepsilon : G \to \widehat{\widehat{G}}$ is an isomorphism.*

Proof. By Theorem 8.2, we have $|G| = |\widehat{G}| = |\widehat{\widehat{G}}|$. Hence it suffices to prove ε is injective. That is, if $g \in G$ with $g \neq 1$, we need to show that there exists some $\chi \in \widehat{G}$ such that $\chi(g) \neq 1$. Let H be the cyclic group generated by g. By Example 8.1, there is some character $\chi' \in \widehat{H}$ s.t. $\chi'(g) \neq 1$. By Lemma 8.1, χ' extends to a character on G. This completes the proof. □

Theorem 8.4. *Let $n = |G|$ and let $\chi \in \widehat{G}$. Then*

$$\sum_{g \in G} \chi(g) = \begin{cases} n, & \text{if } \chi = 1, \\ 0, & \text{if } \chi \neq 1. \end{cases}$$

Proof. The first equation is obvious. If $\chi \neq 1$, there exists $g_0 \in G$ s.t. $\chi(g_0) \neq 1$. Then we have

$$\chi(g_0)\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(g_0 g) = \sum_{g\in G}\chi(g).$$

Since $\chi(g_0) \neq 1$, this implies

$$\sum_{g\in G}\chi(g) = 0.$$

□

Corollary 8.5. *Let $n = |G|$ and let $g \in G$. Then*

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

Proof. It follows from Theorem 8.4 and Theorem 8.3. □

8.2 Dirichlet L-functions

Let $q \in \mathbb{N}^*$. Denote by $G(q)$ the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$.

Definition 8.3. *An element χ of $\widehat{G(q)}$ is called a **Dirichlet character** modulo q. It can be viewed as an arithmetic function via*

$$\chi(n) = \begin{cases} \chi(n \bmod q), & (q,n) = 1, \\ 0, & (q,n) > 1. \end{cases}$$

*The arithmetic function induced by the trivial character, is called the **principal character** and is usually denoted by χ_0.*

Proposition 8.6. *Let χ be a Dirichlet character modulo q. Then χ is a completely multiplicative periodic function with period q.*

Proof. It is clear. □

Let q be an integer ≥ 1 and let χ be a Dirichlet character modulo q. We define the **Dirichlet L-function** by the Dirichlet series

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

Since $|\chi(n)| \leq 1$, this series is absolutely convergent in the half-plane $\operatorname{Re} s > 1$. By Theorem 5.6, in this region, we have

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

Lemma 8.7. *Let χ be a Dirichlet character modulo q. If $\chi \neq \chi_0$, we have*

$$\left|\sum_{n\leq x} \chi(n)\right| \leq \varphi(q)$$

for any $x \geq 1$.

Proof. It follows directly from the orthogonality of characters (Theorem 8.4) and the periodicity of χ. □

Proposition 8.8. *Let χ be a Dirichlet character modulo q. If $\chi \neq \chi_0$, the series $L(s,\chi)$ is convergent in the half-plane $\operatorname{Re} s > 0$.*

Proof. By partial summation, we have

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = s\int_1^{\infty} \frac{1}{t^{s+1}} \sum_{n\leq t} \chi(n)\,\mathrm{d}t.$$

By Lemma 8.7, the sum $\sum_{n\leq t}\chi(n)$ is bounded. So the last integral is absolutely convergent in $\operatorname{Re} s > 0$. □

Proposition 8.9. *For $\chi = \chi_0 (\bmod q)$ and $\operatorname{Re} s > 1$, one has*

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

Hence the analytic continuation of $\zeta(s)$ gives that of $L(s,\chi_0)$.

Proof. It is clear. □

8.3 The non-vanishing of $L(1, \chi)$

Now we are going to prove there are infinitely many prime numbers in the arithmetic progression $\{kq + a\}_{k\in\mathbb{Z}}$. The key point is to show that $L(1, \chi) \neq 0$. Throughout this section, χ stands for a character modulo q.

Let p be a prime number not dividing q. Let $f(p)$ denote the order of the image of p in $G(q)$. Let $g(p) = \varphi(q)/f(p)$. In other words, $f(p)$ is the order of the subgroup of $G(q)$ generated by p and $g(p)$ is the index of this subgroup.

Lemma 8.10. *If $p \nmid q$, one has the identity*

$$\prod_{\chi \bmod q} (1 - \chi(p)T) = \left(1 - T^{f(p)}\right)^{g(p)}.$$

Proof. Let W be the set of $f(p)$-th roots of unity. One has

$$\prod_{w\in W} (1 - wT) = 1 - T^{f(p)}.$$

By Example 8.1 and Lemma 8.1, for each $w \in W$, the number of characters $\chi \in \widehat{G(q)}$ such that $\chi(p) = w$ is $g(p)$ [1]. So the desired conclusion follows. □

Notation. Write

$$Z_q(s) = \prod_{\chi \bmod q} L(s, \chi).$$

Lemma 8.11. *One has*

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

This is a Dirichlet series, with non-negative integral coefficients, converging in the half-plane $\operatorname{Re} s > 1$.

[1] Let H be the subgroup of $G(q)$ generated by p. Since we have the exact sequence

$$1 \to \widehat{G(q)/H} \to \widehat{G(q)} \to \widehat{H} \to 1,$$

for each $\chi \in \widehat{H}$, there are exactly $\varphi(q)/f(p) = g(p)$ preimages in $\widehat{G(q)}$.

Proof. The product expansion follows from Lemma 8.10 with $T = p^{-s}$. Since

$$\left(1 - \frac{1}{p^{f(p)s}}\right)^{-1} = 1 + \frac{1}{p^{f(p)s}} + \frac{1}{p^{2f(p)s}} + \cdots,$$

the second assertion is clear. □

Now we are going to show that $L(1,\chi) \neq 0$. Note that $s = 1$ is a simple pole of $L(s,\chi_0)$. If $L(1,\chi) = 0$ for some $\chi \neq \chi_0$,

$$Z_q(s) = \prod_{\chi \bmod q} L(s,\chi)$$

will be holomorphic at $s = 1$. The following lemma tells us that if it is the caase, the Dirichlet series of $Z_q(s)$ will converge for $\operatorname{Re} s > 0$.

Lemma 8.12. *Let*

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

be a Dirichlet series with $f(n) \geq 0$. Suppose that $D(f;s)$ converges for $\operatorname{Re} s > \sigma$ for some $\sigma \in \mathbb{R}$. If $D(f;s)$ can be analytically continuated to a neighborhood of $s = \sigma$, then there exists a number $\varepsilon > 0$ such that $D(f;s)$ converges for $\operatorname{Re} s > \sigma - \varepsilon$.

Proof. Without loss of generality, we assume $\sigma = 0$. For $\operatorname{Re} s > 0$, we have

$$D^{(k)}(f;s) = (-1)^k \sum_{n=1}^{\infty} \frac{(\log n)^k f(n)}{n^s}.$$

Since $D(f;s)$ is holomorphic near $s = 0$, it is holomorphic in the disc $|s-1| \leq 1+\varepsilon$ for some $\varepsilon > 0$. In particular, its Taylor series converges in this disc. So we can write

$$D(f;s) = \sum_{k=0}^{\infty} \frac{D^{(k)}(f;1)}{k!}(s-1)^k$$

in this disc. Taking $s = -\varepsilon$, we obtain that

$$\begin{aligned} D(f;-\varepsilon) &= \sum_{k=0}^{\infty} \frac{(1+\varepsilon)^k}{k!}(-1)^k D^{(k)}(f;1) \\ &= \sum_{k=0}^{\infty} \frac{(1+\varepsilon)^k}{k!} \sum_{n=1}^{\infty} \frac{(\log n)^k f(n)}{n} \\ &= \sum_{k=0}^{\infty} \sum_{n=1}^{\infty} \frac{(1+\varepsilon)^k (\log n)^k f(n)}{nk!}. \end{aligned}$$

Since the coefficients of this double series is non-negative, we can freely rearranging terms. So the following series is convergent:

$$\sum_{n=1}^{\infty} \frac{f(n)}{n} \sum_{k=0}^{\infty} \frac{(1+\varepsilon)\log n)^k}{k!} = \sum_{n=1}^{\infty} \frac{f(n)}{n} \exp\left((1+\varepsilon)\log n\right) = \sum_{n=1}^{\infty} \frac{f(n)}{n^{-\varepsilon}}.$$

So the series $D(f;s)$ is actually convergent at $s=-\varepsilon$ hence is convergent for all s with $\operatorname{Re} s \geq -\varepsilon$. □

Theorem 8.13. *$L(1,\chi) \neq 0$ for all $\chi \neq \chi_0$.*

Proof. Suppose on the contrary that $L(1,\chi)=0$ for some $\chi \neq \chi_0$. Then $Z_q(s)$ is holomorphic at $s=1$ hence is holomorphic in $\operatorname{Re} s > 0$. By Lemma 8.12 and Lemma 8.11, its Dirichlet series would converge in the same region. However, this is impossible. By Lemma 8.11, the p-factor of $Z_q(\sigma)$ is

$$\left(1-\frac{1}{p^{f(p)\sigma}}\right)^{-g(p)} = \left(1+\frac{1}{p^{f(p)\sigma}}+\frac{1}{p^{2f(p)\sigma}}+\cdots\right)^{g(p)} \geq \sum_{k=0}^{\infty} \frac{1}{p^{k\sigma\varphi(q)}},$$

where we have used the fact that $f(p)g(p)=\varphi(q)$. So by taking $\sigma = 1/\varphi(q)$, we have

$$Z_q\left(\frac{1}{\varphi(q)}\right) \geq \sum_{\substack{n=1 \\ (n,q)=1}}^{\infty} \frac{1}{n} = +\infty.$$

That is, the Dirichlet series of $Z_q(s)$ diverges at $s=1/\varphi(q)$. This is a contradiction. □

8.4 Primes in arithmetic progressions

In this section, we will prove Dirichlet's theorem, which states that there are infinitely many prime numbers in the arithmetic progression $\{kq+a\}_{k\in\mathbb{Z}}$ provided that $(a,q)=1$. We will actually prove a stronger result that the (analytic) density of primes in this progression is $1/\varphi(q)$.

Definition 8.4 (Analytic density)**.** *Let $\mathcal{A} \subseteq \mathbb{P}$. The (Dirichlet) analytic density of $\mathcal{A}$ is defined by the limit (if exists)*

$$\lim_{\sigma\to 1^+} \left(\sum_{p\in\mathcal{A}} \frac{1}{p^\sigma}\right) \Big/ \left(\sum_{p\in\mathbb{P}} \frac{1}{p^\sigma}\right).$$

Theorem 8.14. *Let $(a, q) = 1$. Let $\mathbb{P}_{q,a}$ be the set of prime numbers p such that*

$$p \equiv a \pmod{q}.$$

Then the analytic density of $\mathbb{P}_{q,a}$ is $1/\varphi(q)$.

Corollary 8.15 (Dirichlet)**.** *The set $\mathbb{P}_{q,a}$ is infinite.*

Notation. For $\chi \bmod q$, put

$$f_\chi(s) = \sum_p \frac{\chi(p)}{p^s}, \quad \operatorname{Re} s > 1.$$

Lemma 8.16. *Let $\sigma > 1$. For $\chi = \chi_0$, we have*

$$f_{\chi_0}(\sigma) \sim \log \frac{1}{\sigma - 1}$$

as $\sigma \to 1^+$. For $\chi \neq \chi_0$, $f_\chi(\sigma)$ is bounded as $\sigma \to 1^+$.

Proof. For $\chi = \chi_0$, we have

$$f_{\chi_0}(\sigma) = \sum_{p \nmid q} \frac{1}{p^\sigma} = \sum_p \frac{1}{p^\sigma} + O(1).$$

By the Euler product of $\zeta(s)$ (Corollary 5.7), one has

$$\log \zeta(\sigma) = -\sum_p \log\left(1 - \frac{1}{p^\sigma}\right) = \sum_p \frac{1}{p^\sigma} + O(1).$$

Since $s = 1$ is a simple pole of $\zeta(s)$, we have

$$\log \zeta(\sigma) \sim \log \frac{1}{\sigma - 1}$$

as $\sigma \to 1^+$. So

$$f_{\chi_0}(\sigma) = \log \zeta(\sigma) + O(1) \sim \log \frac{1}{\sigma - 1}$$

as $\sigma \to 1^+$. For $\chi \neq \chi_0$, we consider

$$\log L(\sigma, \chi) = -\sum_p \log\left(1 - \frac{\chi(p)}{p^\sigma}\right) = \sum_p \frac{\chi(p)}{p^\sigma} + O(1) = f_\chi(\sigma) + O(1).$$

Since $L(s, \chi)$ is holomirphic at $s = 1$, $f_\chi(\sigma)$ is bounded as $\sigma \to 1^+$. □

Proof of Theorem 8.14. We investigate the behaviour of

$$g_a(\sigma) = \sum_{p \equiv a(\bmod q)} \frac{1}{p^\sigma}$$

as $\sigma \to 1^+$. By the orhogonality of characters, we have

$$g_a(\sigma) = \sum_p \frac{1}{p^\sigma} \left(\frac{1}{\varphi(q)} \sum_{\chi \bmod q} \chi(a^{-1})\chi(p) \right) = \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \chi(a)^{-1} f_\chi(\sigma).$$

By Lemma 8.16, as $\sigma \to 1^+$, the right side of the above equation

$$\sim \frac{1}{\varphi(q)} \log \frac{1}{\sigma - 1} \sim \frac{1}{\varphi(q)} \sum_p \frac{1}{p^\sigma}.$$

□