11. Dirichlet characters

Our next goal is Dirichlet's theorem on primes in arithmetic progression, for which we need some algebra.

Definition 11.1. Let G be a group. A *character* of G is a group homomorphism $\chi : G \to \mathbb{C}^*$, where $\mathbb{C}^*$ is the multiplicative group of non-zero complex numbers. The set of characters of G is written $\hat{G}$.

By homomorphy we have $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in G$ and $\chi(e_G) = 1$, where e_G is the identity element of G. We denote by $\chi_0 \in \hat{G}$ the *trivial character*

$$\chi_0(a) = 1, \qquad \text{for all } a \in G.$$

(This is sometimes called the *principal character*.) We henceforth assume that G is finite.

Lemma 11.2. *If G is finite then $\hat{G}$ is also a finite group.*

Proof. Let $g \in G$, which by assumption has finite order; i.e. $g^n = e_G$ for some $n \in \mathbb{N}$. Then $1 = \chi(e_G) = \chi(g^n) = \chi(g)^n$. Hence $|\chi(g)| = 1$ and $\chi(g)$ is an nth root of unity. Moreover, $n = \text{ord}(g) \mid \#G$.

For $\chi_1, \chi_2 \in \hat{G}$ define $\chi_1\chi_2$ by $\chi_1\chi_2(a) = \chi_1(a)\chi_2(a)$ for all $a \in G$. Clearly $\chi_1\chi_2 \in \hat{G}$. Moreover, if $\chi \in \hat{G}$ then also $\bar{\chi} \in \hat{G}$ (where $\bar{\chi}(a) := \overline{\chi(a)}$) and $\chi\bar{\chi}(a) = \chi(a)\overline{\chi(a)} = |\chi(a)|^2 = 1$, for all $a \in G$. Hence $\chi\bar{\chi} = \chi_0$, where χ_0 is the identity of $\hat{G}$. Closure and associativity are obvious and so it follows that $\hat{G}$ is a group. Finally, it is a finite group since since $\chi(a)$ is a $(\#G)$th root of unity for all $\chi \in \hat{G}$ and for all $a \in G$. ☐

A useful property of characters is encoded in the following definition.

Definition 11.3. Let G be a finite group. We say that G *has orthogonality of characters* if

$$\sum_{g \in G} \chi(g) = \begin{cases} \#G & \text{if } \chi = \chi_0, \\ 0 & \text{if } \chi \neq \chi_0, \end{cases}$$

and

$$\sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} \#\hat{G} & \text{if } g = e_G, \\ 0 & \text{if } g \neq e_G, \end{cases}$$

This property is enjoyed by all finite cyclic groups, as the following result shows.

Theorem 11.4. *Assume that G is a finite cyclic group of order n, generated by a. Then:*

(1) *$\hat{G}$ has exactly n elements*

$$\chi_k(a^m) = e\left(\frac{km}{n}\right), \qquad k = 1, \ldots, n,$$

where $e(x) = \exp(2\pi i x)$.

(2) *G has orthogonality of characters.*

(3) *$\hat{G}$ is a cyclic group and it is generated by χ_1 (so $G \cong \hat{G}$).*

Proof. Let $\chi \in \hat{G}$. Then $\chi(a) = e(k/n)$ for some $k \in \{1, \dots, n\}$. Hence

$$\chi(a^m) = \chi(a)^m = e\left(\frac{km}{n}\right),$$

proving part (1), since all n characters are distinct.

By (1) $\hat{G}$ is cyclic and generated by χ_1, so $G \cong \hat{G}$, as required for part (3).

To prove (2) we need to check the identities in Definition 11.3. We show that

$$\sum_{g \in G} \chi(g) = \begin{cases} \#G & \text{if } \chi = \chi_0, \\ 0 & \text{if } \chi \neq \chi_0. \end{cases}$$

This is trivial for $\chi = \chi_0$, so suppose that $1 \leq k \leq n-1$. Then

$$\sum_{g \in G} \chi(g) = \sum_{m=0}^{n-1} \chi_k(a^m) = \sum_{m=0}^{n-1} e\left(\frac{km}{n}\right) = \frac{1 - e(kn/n)}{1 - e(k/n)} = 0,$$

as required. Finally the remaining identity follows from this one by by duality. ☐

Lemma 11.5. *Let G_1, G_2 be finite cyclic groups and let $G = G_1 \times G_2$. Let $\chi_i \in \hat{G}_i$ for $i = 1, 2$ and define $\chi : G \to \mathbb{C}^*$ via $\chi(g_1, g_2) = \chi_1(g_1)\chi_2(g_2)$. This is a character. Conversely, if $\chi \in \hat{G}$ then there exists a unique choice of $\chi_1 \in \hat{G}_1$ and $\chi_2 \in \hat{G}_2$ such that $\chi(g) = \chi_1(g_1)\chi_2(g_2)$. Furthermore, G has orthogonality of characters and $\hat{G} \cong \hat{G}_1 \times \hat{G}_2$.*

Proof. Recall from Theorem 11.4 that G_1 and G_2 both have orthogonality of characters. We confirm the claims:

- It is clear that χ is a character.
- To check the converse, let $\chi \in \hat{G}$ and define $\chi_i \in \hat{G}_i$ by $\chi_1(g_1) = \chi(g_1, e_{G_2})$ and $\chi_2(g_2) = \chi(e_{G_1}, g_2)$. Then clearly $\chi = \chi_1\chi_2$ and $\chi \in \hat{G}$. Moreover, the χ_i are unique: if $g = (g_1, e_{G_2})$ then
$$\chi(g) = \chi(g_1, e_{G_2}) = \chi_1(g_1)\chi_2(e_{G_2}) = \chi_1(g_1).$$
Similarly for $\chi_2(g_2)$.
- $$\sum_{g \in G} \chi(g) = \sum_{g_1 \in G_1} \chi_1(g_1) \sum_{g_2 \in G_2} \chi_2(g_2) = \begin{cases} \#G_1 \#G_2 & \text{if } \chi_1 = \chi_0 \text{ and } \chi_2 = \chi_0, \\ 0 & \text{otherwise.} \end{cases}$$
- $$\sum_{\chi \in \hat{G}} \chi(g) = \sum_{\chi_1 \in \hat{G}_1} \chi_1(g_1) \sum_{\chi_2 \in \hat{G}_2} \chi_2(g_2) = \begin{cases} \#G_1 \#G_2 & \text{if } g = (e_{G_1}, e_{G_2}) = e_G, \\ 0 & \text{otherwise.} \end{cases}$$
- It is clear that $\hat{G} \cong \hat{G}_1 \times \hat{G}_2$.

☐

Corollary 11.6. *Let G be a finite abelian group. Then $G \cong \hat{G}$ and G has orthogonality of characters.*

Proof. The fundamental theorem of abelian groups implies that $G \cong C_1 \times \cdots \times C_r$ for suitable cyclic groups $C_1, \dots, C_r$. Now apply Lemma 11.5 repeatedly. ☐

We now come to the particular characters that will occupy our attention for some time to come.

Definition 11.7. (1) Let $q \in \mathbb{N}$. A *Dirichlet character mod q* is a character of the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^*$.

(2) If χ is a Dirichlet character mod q, we extend χ to an arithmetic function $\chi : \mathbb{Z} \to \mathbb{C}$ via

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

Hence a Dirichlet character mod q is a completely multiplicative arithmetic function $\chi : \mathbb{Z} \to \mathbb{C}$ of period q such that $\chi(n) = 0$ if $(n,q) > 1$. Conversely, any such function is a Dirichlet character mod q. Corollary 11.6 implies that the number of Dirichlet characters mod q is $\varphi(q)$. The trivial Dirichlet character is given by

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

Further examples:

(1) $q = 4$. Then there are $\varphi(q) = \varphi(4) = 2$ Dirichlet characters mod 4. These are χ_0 and χ_1, where

$$\chi_1(n) = \begin{cases} +1 & \text{if } n \equiv 1 \bmod 4, \\ -1 & \text{if } n \equiv 3 \bmod 4, \\ 0 & \text{if } 2 \mid n. \end{cases}$$

(2) $q = p > 2$ a prime. Then $\chi(n) = (\frac{n}{p})$ is a Dirichlet character mod p.

The following result is a direct consequence of Corollary 11.6:

Corollary 11.8 (Orthogonality of Dirichlet characters)**.** *Let $q \in \mathbb{N}$. Then*

$$\sum_{\substack{n=1 \\ (n,q)=1}}^{q} \chi(n) = \begin{cases} \varphi(q) & \textit{if } \chi = \chi_0, \\ 0 & \textit{if } \chi \neq \chi_0, \end{cases}$$

and

$$\sum_{\chi \bmod q} \chi(n) = \begin{cases} \varphi(q) & \textit{if } n \equiv 1 \bmod q, \\ 0 & \textit{otherwise,} \end{cases}$$

where the latter sum is over all Dirichlet characters mod q.

The following result is very useful for detecting congruence conditions in counting problems.

Corollary 11.9. *Let $q \in \mathbb{N}$ and let $a \in \mathbb{Z}$ such that $(a,q) = 1$. Then for any $n \in \mathbb{Z}$ we have*

$$\frac{1}{\varphi} \sum_{\chi \bmod q} \bar{\chi}(a)\chi(n) = \begin{cases} 1 & \textit{if } n \equiv a \bmod q, \\ 0 & \textit{otherwise.} \end{cases}$$

We now distinguish between "primitive" and "imprimitive" Dirichlet characters mod q. Suppose $d \mid q$ and let χ^* be a character mod d. Put

$$\chi(n) = \begin{cases} \chi^*(n) & \text{if } (n,q) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Then χ is a Dirichlet character mod q. In this situation we say that χ^* *induces* χ.

Remark. If there is a prime $p \mid q$ such that $p \nmid d$ then χ does not have period d. If q and d share the same primes factors then $\chi(n) = \chi^*(n)$ for all n.

Definition 11.10. Let χ be a character mod q. We say d is a *quasiperiod* of χ if $\chi(m) = \chi(n)$ whenever $m \equiv n \bmod d$ and $(mn, q) = 1$. The least quasiperiod of χ is called the *conductor of* χ.

Lemma 11.11. *Let χ be a Dirichlet character mod q. The conductor of χ is a divisor of q.*

Proof. Let d be a quasiperiod of χ and put $g = (d, q)$. We show that g is also a quasiperiod of χ. Suppose $m \equiv n \bmod g$ and $(mn, q) = 1$. Euclid's algorithm implies that there exist $x, y \in \mathbb{Z}$ such that $m - n = dx + qy$. Thus

$$\chi(m) = \chi(m - qy) = \chi(dx + n) = \chi(n).$$

Thus g is a quasiperiod of χ. □

Definition 11.12. A Dirichlet character χ mod q is said to be *primitive* when it has conductor q.

By convention the trivial character χ_0 mod q is imprimitive.

Theorem 11.13. *Let χ be a Dirichlet character mod q with conductor d. Then there exists a unique primitive character χ^* mod d that induces χ.*

Proof. Lemma 11.11 implies that $d \mid q$. Let

$$r = \prod_{\substack{p^a \| q \\ p \nmid d}} p^a.$$

Now let $n \in \mathbb{Z}$. If $(n, q) = 1$ then we define $\chi^*(n) = \chi(n)$. If $(n, q) > 1$ but $(n, d) = 1$ we choose any $k \in \mathbb{Z}$ such that $(n + kd, q) = 1$ and define

$$\chi^*(n) = \chi(n + kd).$$

Note that such an integer exists, for it suffices to have $(n + kd, r) = 1$. (To see this we choose $a \in (\mathbb{Z}/r\mathbb{Z})^*$ and then choose k such that $n + kd \equiv a \bmod r$.) Moreover, we note that although there are many possible choices of k, there is only value of $\chi(n + kd)$ when $(n + kd, q) = 1$. We extend this definition of χ^* by setting $\chi^*(n) = 0$ when $(n, d) > 1$. Then χ^* is a Dirichlet character mod d. If χ_0 is the principle character mod q then

$$\chi(n) = \chi^*(n)\chi_0(n)$$

and so χ^* induces χ. It is clear that χ^* has no quasiperiod less than d, since otherwise so would χ, which contradicts minimality.

It remains to establish uniqueness. Suppose that χ_1 is another character mod d that induces χ. Then, on choosing k as above, for all n with $(n,d)=1$ we have

$$\chi^*(n)=\chi^*(n+kd)=\chi(n+kd)=\chi_1(n+kd)=\chi_1(n),$$

as required. □

The following result gives a useful criterion for primitivity of a Dirichlet character.

Lemma 11.14. *Let χ be a Dirichlet character mod q. The following are equivalent:*

(1) *χ is primitive;*
(2) *if $d \mid q$, with $d<q$, then there exists an integer $c \equiv 1 \bmod d$ which is coprime to q such that $\chi(c) \neq 1$;*
(3) *if $d \mid q$, with $d<q$, then for any $a \in \mathbb{Z}$ we have*

$$\sum_{\substack{n=1\\ n\equiv a \bmod d}}^{q} \chi(n)=0.$$

Proof. (1) ⇒ (2): Suppose $d \mid q$ with $d<q$. Since χ is primitive there exist $m,n \in \mathbb{Z}$ such that $m \equiv n \bmod d$, with $\chi(m) \neq \chi(n)$ and $\chi(mn) \neq 0$. Choose c coprime to q such that $cm \equiv n \bmod q$.

(2) ⇒ (3): Let c be as in (2). As k runs over residues modulo q/d, the numbers $n=ac+kcd$ run through all residues modulo q for which $n \equiv a \bmod d$. Thus the sum is

$$S=\sum_{\substack{n=1\\ n\equiv a \bmod d}}^{q} \chi(n)=\sum_{k=1}^{q/d}\chi(ac+kcd)=\chi(c)S.$$

Hence $S=0$ since $\chi(c)\neq 0$.

(3) ⇒ (1): Suppose $d \mid q$ with $d<q$. Take $a=1$ in (3). Then $\chi(1)=1$ is one term in the sum. But the sum is zero and so there exists another term $\chi(n)$ such that $\chi(n)\neq 1$ and $\chi(n)\neq 0$. But $n\equiv 1 \bmod d$ and so d is not a quasiperiod of χ. This implies that χ is primitive. □

Lemma 11.15. *Suppose that $(q_1,q_2)=1$ and let χ_i be a Dirichlet character mod q_i for $i=1,2$. Then $\chi=\chi_1\chi_2$ is primitive mod q_1q_2 if and only if χ_1 and χ_2 are both primitive.*

Proof. Let $q=q_1q_2$.

"⇒" Let d_i be the conductor of χ_i. If $(mn,q)=1$ and $m\equiv n \bmod d_1d_2$ then $\chi_i(m)=\chi_i(n)$ and hence d_1d_2 is a quasiperiod of χ. Thus $d_1d_2=q$ since χ is primitive. Thus $d_1=q_1$ and $d_2=q_2$ since $d_i \mid q_i$ for $i=1,2$.

"⇐" Let d be the conductor of χ and put $d_i=(d,q_i)$. We show that d_1 is a quasiperiod of χ_1. Suppose $(mn,q_1)=1$ and $m\equiv n \bmod d_1$. Choose $m',n'\in\mathbb{Z}$ such that

$$m'\equiv m \bmod q_1,\quad m'\equiv 1 \bmod q_2,\quad n'\equiv n \bmod q_1,\quad n'\equiv 1 \bmod q_2.$$

Thus $m'\equiv n' \bmod d$ and $(m'n',q)=1$. It follows that $\chi(m')=\chi(n')$. But $\chi(m')=\chi_1(m)$ and $\chi(n')=\chi_1(n)$, whence $\chi_1(m)=\chi_1(n)$ and so d_1 is a quasiperiod of χ_1. Since χ_1 is primitive this implies that $d_1=q_1$. Similarly, $d_2=q_2$, whence $d=q$.

□

If one wants to classify primitive Dirichlet characters the latter result implies that it suffices to determine the primitive characters mod p^a. Let χ be a character mod p^a.

Suppose first that $p > 2$ and let g be a primitive root of p^a (i.e. a generator for the cyclic group $(\mathbb{Z}/p^a\mathbb{Z})^*$). Then according to Theorem 11.4 we have

$$\chi(n) = e\left(\frac{k \operatorname{ind}_g(n)}{\varphi(p^a)}\right), \qquad \text{for some } k \in \mathbb{Z},$$

where $\operatorname{ind}_g(n)$ is the *index* of n, defined via $n = g^{\operatorname{ind}_g(n)}$. We now argue according to the value of a:

$a = 1$: χ is primitive if and only if $\chi \neq \chi_0$. (This is if and only if $(p-1) \nmid k$.)

$a > 1$: χ is primitive if and only if $p \nmid k$. (The only proper divisor of p^a is p^b for $0 \leq b < a$, and $e(k \operatorname{ind}_g(n)/\varphi(p^a)) = e(k' \operatorname{ind}_g(n)/\varphi(p^b))$ if and only if $p \mid k$.)

Next we suppose that $p = 2$.

$a = 1$: We have only the trivial character χ_0, which is imprimitive.

$a = 2$: We have already seen that there are two characters χ_0 (imprimitive) and χ_1 (primitive).

$a > 2$: The analysis of this case is a bit more complicated since there is no primitive root of 2^a when $a \geq 3$. However, for any $n \in (\mathbb{Z}/2^a\mathbb{Z})^*$ there exists $\mu \in \mathbb{Z}/2\mathbb{Z}$ and $\nu \in \mathbb{Z}/2^{a-2}\mathbb{Z}$ such that $n \equiv (-1)^\mu 5^\nu \bmod 2^a$. Dirichlet characters mod 2^a take the form

$$\chi(n) = e\left(\frac{j\mu}{2} + \frac{k\nu}{2^{a-2}}\right),$$

for $j \in \mathbb{Z}/2\mathbb{Z}$ and $k \in \mathbb{Z}/2^{a-2}\mathbb{Z}$. (Note that the number of Dirichlet characters mod 2^a is $\varphi(2^a) = 2^{a-1}$.) One finds that χ is primitive if and only if k is odd.

Exercise. What are the *real* primitive characters mod p^a?

We know that there are $\varphi(q)$ Dirichlet characters mod q. We can now calculate the number $\varpi(q)$ of primitive Dirichlet characters mod q.

Lemma 11.16. $\varpi(q) = q \prod_{p \| q}(1 - \frac{2}{p}) \prod_{p^2 | q}(1 - \frac{1}{p})^2$.

Proof. By Lemma 11.15 we have $\varpi(q) = \prod_{p^a \| q} \varpi(p^a)$. The argument is now a case by case analysis. For example, when $p > 2$ and $a = 1$, we saw that the number of primitive characters mod p is equal to the number of $k \in \mathbb{Z}/p\mathbb{Z}$ such that $(p-1) \nmid k$, which is $p - 1 - 1 = p - 2$. The remaining details are an exercise. □