MATH 571 CHAPTER 2

1. The multiplicative structure of residue classes

In elementary number theory courses it is usual taught that the reduced residue classes modulo q form a cyclic group under multiplication if and only if $q = p^k$ with $p = 2$ and $k = 1$ or 2, or with $p > 2$ and all $k \geq 1$. A generator g is called a primitive root. It is often also shown that if $p = 2$ and $k \geq 3$, then every reduced residue modulo 2^k is generated by

$$(-1)^u 5^v$$

where $u = 0$ or 1 and $0 \leq v < 2^{k-2}$. One can then use the Chinese Remainder Theorem to express each residue modulo q in a suitable form. This was all first proved by Gauss. It is also an example of the theorem, usually proved in abstract algebra courses, that each abelian group is a direct product of cyclic groups. The methods of abstract algebra do not necessarily give explicit representations. We will not need this later, but it comes up in the next section.

2. Dirichlet characters

It is often useful to represent the characteristic function of a reduced residue class (mod q) as a linear combination of totally multiplicative functions $\chi(n)$ each one supported on the reduced residue classes and having period q. These are the *Dirichlet characters*. In the fancy language of abstract algebra we are examining the structure of homomorphisms from the units modulo q to an isomorphism of this group on the unit circle in the complex plane. Fundamental is

that the homomorphisms themselves form a group which is also isomorphic to the original group.

Since $\chi(n)$ has period q we may think of it as mapping from residue classes, and since $\chi(n) \neq 0$ if and only if $(n, q) = 1$, we may think of χ as mapping from the multiplicative group of reduced residue classes to the multiplicative group $\mathbb{C}^\times$ of non-zero complex numbers. As χ is totally multiplicative, $\chi(mn) = \chi(m)\chi(n)$ for all m, n, we see that the map $\chi : \left(\mathbb{Z}/q\mathbb{Z}\right)^\times \longrightarrow \mathbb{C}^\times$ is a homomorphism. The method we use to describe these characters applies when $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ is replaced by an arbitrary finite abelian group G, so we consider the slightly more general problem of finding all homomorphisms $\chi : G \to \mathbb{C}^\times$ from such a group G to $\mathbb{C}^\times$. We call these homomorphisms the characters of G, and let $\widehat{G}$ denote the set of all characters of G. We let χ_0 denote the *principal character*, whose value is identically 1. We note that if $\chi \in \widehat{G}$ then $\chi(e) = 1$ where e denotes the identity in G. Let n denote the order of G. If $g \in G$ and $\chi \in \widehat{G}$, then $g^n = e$, and hence $\chi(g^n) = 1$. Consequently $\chi(g)^n = 1$, and so we see that all values taken by characters are n^{th} roots of unity. In particular, this implies that $\widehat{G}$ is finite, since there can be at most n^n such maps. If χ_1 and χ_2 are two characters of G, then we can define a product character $\chi_1\chi_2$ by $\chi_1\chi_2(g) = \chi_1(g)\chi_2(g)$. For $\chi \in \widehat{G}$, let $\overline{\chi}$ be the character $\overline{\chi(g)}$. Then $\chi \cdot \overline{\chi} = \chi_0$, and we see that $\widehat{G}$ is a finite abelian group with identity χ_0. The following lemmas prepare for a full description of $\widehat{G}$ in Theorem 4.

Lemma 2.1. *Suppose that G is cyclic of order n, say $G = (a)$. Then there are exactly n characters of G, namely $\chi_k(a^m) = e(km/n)$ for $1 \le k \le n$. Moreover,*

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

and

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

In this situation, $\widehat{G}$ is cyclic, $\widehat{G} = (\chi_1)$.

Proof. Suppose that $\chi \in \widehat{G}$. As we have observed, $\chi(a)$ is a n^{th} root of unity, say $\chi(a) = e(k/n)$ for some k, $1 \le k \le n$. Hence $\chi(a^m) = \chi(a)^m = e(km/n)$. Since the characters are now known explicitly, the remaining assertions are easily verified. □

Next we describe the characters of the direct product of two groups in terms of the characters of the factors.

Lemma 2.2. *Suppose that G_1 and G_2 are finite abelian groups, and that $G = G_1 \otimes G_2$. If χ_i is a character of G_i, $i = 1, 2$, and $g \in G$ is written $g = (g_1, g_2)$, $g_i \in G_i$, then $\chi(g) = \chi_1(g_1)\chi_2(g_2)$ is a character of G. Conversely, if $\chi \in \widehat{G}$, then there exist unique $\chi_i \in G_i$ such that $\chi(g) = \chi_1(g_1)\chi_2(g_2)$. The identities* 12) *and* 13) *hold for G if they hold for both G_1 and G_2.*

We see here that each $\chi \in \widehat{G}$ corresponds to a pair $(\chi_1, \chi_2) \in \widehat{G}_1 \times \widehat{G}_2$. Thus $G \cong \widehat{G}_1 \otimes \widehat{G}_2$.

Proof. The first assertion is clear. As for the second, put $\chi_1(g_1) = \chi((g_1, e_2))$, $\chi_2(g_2) = \chi((e_1, g_2))$. Then $\chi_i \in \widehat{G}_i$ for $i = 1, 2$, and $\chi_1(g_1)\chi_2(g_2) = \chi(g)$. The χ_i are unique, for if

$g = (g_1, e_2)$ then

$$\chi(g) = \chi((g_1, e_2)) = \chi_1(g_1)\chi_2(e_2) = \chi_1(g_1),$$

and similarly for χ_2. If $\chi(g) = \chi_1(g_1)\chi_2(g_2)$, then

$$\sum_{g \in G} \chi(g) = \Big(\sum_{g_1 \in G_1} \chi_1(g_1) \Big) \Big(\sum_{g_2 \in G_2} \chi_2(g_2) \Big),$$

so that 12) holds for G if it holds for G_1 and for G_2. Similarly, if $g = (g_1, g_2)$, then

$$\sum_{\chi \in \widehat{G}} \chi(g) = \Big(\sum_{\chi_1 \in \widehat{G}_1} \chi_1(g_1) \Big) \Big(\sum_{\chi_1 \in \widehat{G}_2} \chi_2(g_2) \Big),$$

so that (13) holds for G if it holds for G_1 and G_2. □

Theorem 2.3. *Let G be a finite abelian group. Then $\widehat{G}$ is isomorphic to G, and* 12) *and* (13) *both hold.*

Proof. Any finite abelian group is isomorphic to a direct product of cyclic groups, say

$$G \cong C_{n_1} \otimes C_{n_2} \otimes \cdots \otimes C_{n_r}.$$

The result then follows immediately from the lemmas. □

Though G and $\widehat{G}$ are isomorphic, the isomorphism is not canonical. That is, no particular one-to-one correspondence between the elements of G and those of $\widehat{G}$ is naturally distinguished.

Corollary 2.4. *The multiplicative group $\big(\mathbb{Z}/q\mathbb{Z}\big)^\times$ of reduced residue classes* (mod q) *has $\varphi(q)$ Dirichlet characters. If χ is such a character, then*

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

If $(n, q) = 1$ *then*

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

where the sum is extended over the $\varphi(q)$ *Dirichlet characters* $\chi \pmod{q}$.

As we remarked at the outset, for our purposes it is convenient to define the Dirichlet characters (mod q) on all integers; we do this by setting $\chi(n) = 0$ when $(n, q) > 1$. Thus χ is a totally multiplicative function with period q that vanishes whenever $(n, q) > 1$, and any such function is a Dirichlet character (mod q). In this book a character is understood to be a Dirichlet character unless the contrary is indicated.

Corollary 2.5. *If* χ_i *is a character* (mod q_i) *for* $i = 1, 2$, *then* $\chi_1(n)\chi_2(n)$ *is a character* (mod $[q_1, q_2]$). *If* $q = q_1 q_2$, $(q_1, q_2) = 1$, *and* χ *is a character* (mod q), *then there exist unique characters* $\chi_i \pmod{q}$, $i = 1, 2$, *such that* $\chi(n) = \chi_1(n)\chi_2(n)$ *for all* n.

Proof. The first assertion follows immediately from the observations that $\chi_1(n)\chi_2(n)$ is totally multiplicative, that it vanishes if $(n, [q_1, q_2]) > 1$, and that it has period $[q_1, q_2]$. As for the second assertion, we may suppose that $(n, q) = 1$. By the Chinese Remainder Theorem we see that

$$\left(\mathbb{Z}/q\mathbb{Z}\right)^{\times} \cong \left(\mathbb{Z}/q_1\mathbb{Z}\right)^{\times} \otimes \left(\mathbb{Z}/q_2\mathbb{Z}\right)^{\times}$$

if $(q_1, q_2) = 1$. Thus the result follows from Lemma 2. □

Our proof of Theorem 2.3 depends on Abel's Theorem that any finite abelian group is isomorphic to the direct product of cyclic groups, but we can prove Corollary 2.4 without appealing to this result, as follows. By the Chinese

Remainder Theorem we see that

$$\big(\mathbb{Z}/q\mathbb{Z}\big)^\times \cong \bigotimes_{p^\alpha \| q} \big(\mathbb{Z}/p^\alpha\mathbb{Z}\big)^\times.$$

If p is odd then the reduced residue classes (mod p^α) form a cyclic group; in classical language we say there is a primitive root g. Thus if $(n,p)=1$ then there is a unique ν (mod $\varphi(p^\alpha)$) such that $g^\nu \equiv n \pmod{p^\alpha}$. The number ν is called the index of n, and is denoted $\nu = \operatorname{ind}_g n$. From Lemma 2 it follows that the characters (mod p^α), $p>2$, are given by

$$\chi k(n) = e\Big(\frac{k \operatorname{ind}_g n}{\varphi(p^\alpha)}\Big)$$

for $(n,p)=1$. We obtain $\varphi(p^\alpha)$ different characters by allowing k to assume integral values in the range $1 \le k \le \varphi(p^\alpha)$. By Lemma 3 it follows that if q is odd then the general character (mod q) is given by

$$\chi(n) = e\Big(\sum_{p^\alpha \| q} \frac{k \operatorname{ind}_g n}{\varphi(p^\alpha)}\Big)$$

for $(n,q)=1$, where it is understood that $k = k(p^\alpha)$ is determined (mod $\varphi(p^\alpha)$) and that $g = g(p^\alpha)$ is a primitive root (mod p^α).

The multiplicative structure of the reduced residues (mod 2^α) is more complicated. For $\alpha = 1$ or $\alpha = 2$ the group is cyclic (of order 1 or 2, respectively), and (16) holds as before. For $\alpha \ge 3$ the group is not cyclic, but if n is odd then there exist unique $\mu \pmod 2$ and $\nu \pmod{2^{\alpha-2}}$ such that $n \equiv (-1)^\mu 5^\nu \pmod{2^\alpha}$. In group-theoretic terms this means that

$$\big(\mathbb{Z}/2^\alpha\mathbb{Z}\big)^\times \cong C_2 \otimes C_{2^{\alpha-2}}$$

when $\alpha \ge 3$. By Lemma 3 the characters in this case take the form

$$\chi(n) = e\Big(\frac{j\mu}{2} + \frac{k\nu}{2^{\alpha-2}}\Big)$$

for odd n where $j = 0$ or 1 and $1 \le k \le 2^{\alpha-2}$. Thus (17) holds if $8 \nmid q$, but if $8|q$ then the general character takes the form

$$\chi(n) = e\Big(\frac{j\mu}{2} + \frac{k\nu}{2^{\alpha-2}} + \sum_{\substack{p^\alpha \| q \\ p>2}} \frac{\ell \operatorname{ind}_g n}{\varphi(p^\alpha)}\Big)$$

when $(n, q) = 1$.

By definition, if $f(n)$ is totally multiplicative, $f(n) = 0$ whenever $(n, q) > 1$, and $f(n)$ has period q, then f is a Dirichlet character (mod q). It is useful to note that the first condition can be relaxed.

Theorem 2.6. *If f is multiplicative, $f(n) = 0$ whenever $(n, q) > 1$, and f has period q, then f is a Dirichlet character modulo q.*

Proof. It suffices to show that f is totally multiplicative. If $(mn, q) > 1$ then $f(mn) = f(m)f(n)$ since $0 = 0$. Suppose that $(mn, q) = 1$. Hence in particular $(m, q) = 1$, so that the map $k \mapsto n + kq \pmod m$ permutes the residue classes (mod m). Thus there is a k for which $n + kq \equiv 1 \pmod m$, and consequently $(m, n + kq) = 1$. Then

$$\begin{aligned} f(mn) &= f(m(n + kq)) && \text{(by periodicity)} && (2.1)\\ &= f(m)f(n + kq) && \text{(by multiplicativity)} && (2.2)\\ &= f(m)f(n) && \text{(by periodicity),} && (2.3) \end{aligned}$$

and the proof is complete. □

3. Primitive characters

Suppose that $d \mid q$ and that $\chi^\star$ is a character (mod d), and set

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

Then $\chi(n)$ is multiplicative and has period q, so by Theorem 4.7 we deduce that $\chi(n)$ is a Dirichlet character (mod

q). In this situation we say that $\chi^\star$ *induces* χ. If q is composed entirely of primes dividing d then $\chi(n) = \chi^\star(n)$ for all n, but if there is a prime factor of q not found in d then $\chi(n)$ does not have period d. Nevertheless, χ and $\chi^\star$ are nearly the same in the sense that $\chi(p) = \chi^\star(p)$ for all but at most finitely many primes, and hence

$$L(s,\chi) = L(s,\chi^\star)\prod_{p|q}\Big(1-\frac{\chi^\star(p)}{p^s}\Big).$$

Our immediate task is to determine when one character induces another.

Lemma 3.1. *Let χ be a character* (mod q). *We say that d is a* quasiperiod *of χ if $\chi(m) = \chi(n)$ whenever $m \equiv n \pmod d$ and $(mn, q) = 1$. The least quasiperiod 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 that $m \equiv n \pmod g$ and that $(mn, q) = 1$. Since g is a linear combination of d and q, and $m - n$ is a multiple of g, it follows that there are integers x and y such that $m - n = dx + qy$. Then $\chi(m) = \chi(m - qy) = \chi(n + dx) = \chi(n)$. Thus g is a quasiperiod of χ. □

With more effort it can be shown that if d_1 and d_2 are quasiperiods of χ then (d_1, d_2) is also a quasiperiod, and hence the least quasiperiod divides all other quasiperiods, and in particular it divides q (since q is a quasiperiod of χ).

The least quasiperiod d of χ is called the *conductor* of χ. Suppose that d is the conductor of χ. If $(n, d) = 1$ then $(n + kd, d) = 1$. Also, if $(r, d) = 1$ then there exist values of $k \pmod r$ for which $(n + kd, r) = 1$. Hence there exist integers k for which $(n + kd, q) = 1$. For such a k put

$\chi^\star(n) = \chi(n+kd)$. Although there are many such k, there is only one value of $\chi(n+kd)$ when $(n+kd, q) = 1$. We extend the definition of $\chi^\star$ by setting $\chi^\star(n) = 0$ when $(n, d) > 1$. It is readily seen that $\chi^\star$ is multiplicative and that $\chi^\star$ has period d. Thus by Theorem 4.7, $\chi^\star$ is a character modulo d. Moreover, if χ_0 is the principal character modulo q, then $\chi(n) = \chi^\star(n)\chi_0(n)$. Thus $\chi^\star$ induces χ. Clearly $\chi^\star$ has no quasiperiod smaller than d, for otherwise χ would have a smaller quasiperiod, contradicting the minimality of d. In addition, $\chi^\star$ is the only character (mod d) that induces χ, for if there were another, say χ_1, then for any n with $(n, d) = 1$ we would have $\chi^\star(n) = \chi^\star(n + kd) = \chi(n + kd) = \chi_1(n + kd) = \chi_1(n)$, on choosing k as above.

A character χ modulo q is said to be *primitive* when q is the least quasiperiod of χ. Such χ are not induced by any character having a smaller conductor. We summarize our discussion as follows.

Theorem 3.2. *Let χ denote a Dirichlet character modulo q and let d be the conductor of χ. Then $d \mid q$, and there is a unique primitive character $\chi^\star$ modulo d that induces q.*

We now identify the primitive characters in such a way that we can describe them in terms of the explicit construction of §5.2.

Lemma 3.3. *Suppose that $(q_1, q_2) = 1$ and that χ_1 and χ_2 are characters modulo q_1 and q_2 respectively. Put $\chi(n) = \chi_1(n)\chi_2(n)$. Then the character χ is primitive modulo q_1q_2 if and only if both χ_1 and χ_2 are primitive.*

Proof. For convenience write $q = q1q_2$. Suppose that χ is primitive modulo q, and for $i = 1, 2$ let d_i be the conductor of χ_i. If $(mn, q) = 1$ and $m \equiv n \pmod{d_1d_2}$ then $\chi_i(m) = \chi_i(n)$ for $i = 1, 2$, and hence d_1d_2 is a quasiperiod of χ. Since χ is primitive, this means that $d_1d_2 = q$. But $d_i \mid$

q_i, so this implies that $d_i = q_i$, which is to say that the characters χ_i are primitive.

Now suppose that χ_i is primitive modulo q_i for $i = 1, 2$, and let d be the conductor of χ. Put $d_i = (d, q_i)$. We show that d_1 is a quasiperiod of χ_1. Suppose that $m \equiv n \pmod{d_1}$ and that $(mn, q_1) = 1$. Choose m' so that $m' \equiv m \pmod{q_1}$, $m' \equiv 1 \pmod{q_2}$. Similarly, choose n' so that $n' \equiv n \pmod{q_1}$ and $n' \equiv 1 \pmod{q_2}$. Thus $m' \equiv n' \pmod{d}$ and $(m'n', q) = 1$, and hence $\chi(m') = \chi(n')$. But $\chi(m') = \chi_1(m)$ and $\chi(n') = \chi_1(n)$, so $\chi_1(m) = \chi_1(n)$. Thus d_1 is a quasiperiod of χ_1. Since χ_1 is primitive, it follows that $d_1 = q_1$. Similarly $d_2 = q_2$. Thus $d = q$, which is to say that χ is primitive. □

By Lemma 3.3 we see that in order to exhibit the primitive characters explicitly it suffices to determine the primitive characters (mod p^α). Suppose first that p is odd, and let g be a primitive root of p^α. Then by (4.16) we know that any character $\chi \pmod{p^\alpha}$ is given by

$$\chi(n) = e\Big(\frac{k \operatorname{ind}_g n}{\varphi(p^\alpha)}\Big)$$

for some integer k. If $\alpha = 1$ then χ is primitive if and only if it is non-principal, which is to say that $(p-1) \nmid k$. If $\alpha > 1$ then χ is primitive if and only if $p \nmid k$. Now consider primitive characters (mod 2^α). When $\alpha = 1$ we have only the principal character, which is imprimitive. When $\alpha = 2$ we have two characters, namely the principal character, which is imprimitive, and the primitive character χ given by $\chi(4k+1) = 1$, $\chi(4k-1) = -1$. When $\alpha \geq 3$, we write an odd integer n in the form $n \equiv (-1)^\mu 5^\nu \pmod{2^\alpha}$, and then characters (mod 2^α) are of the form

$$\chi(n) = e\Big(\frac{j\mu}{2} + \frac{k\nu}{2^{\alpha-2}}\Big)$$

where j is determined (mod 2) and k is determined (mod $2^{\alpha-2}$). Here χ is primitive if and only if k is odd.

We now give two useful criteria for primitivity.

Theorem 3.4. *Let χ be a character modulo q. Then the following are equivalent:*
(1) χ is primitive.
(2) If $d \mid q$ and $d < q$ then there is a c such that $c \equiv 1 \pmod{d}$, $(c, q) = 1$, $\chi(c) \neq 1$.
(3) If $d \mid q$ and $d < q$, then for every integer a,

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

Proof. (1) $\Rightarrow$ (2). Suppose that $d \mid q$, $d < q$. Since χ is primitive, there exist integers m and n such that $m \equiv n \pmod{d}$, $\chi(m) \neq \chi(n)$, $\chi(mn) \neq 0$. Choose c so that $(c, q) = 1$, $cm \equiv n \pmod{q}$. Thus we have (2).

(2) $\Rightarrow$ (3). Let c be as in (2). As k runs through a complete residue system (mod q/d), the numbers $n = ac + kcd$ run through all residues (mod q) for which $n \equiv a \pmod{d}$. Thus the sum S in question is

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

Since $\chi(c) \neq 1$, it follows that $S = 0$.

(3) $\Rightarrow$ (1). Suppose that $d \mid q$, $d < q$. Take $a = 1$ in (3). Then $\chi(1) = 1$ is one term in the sum, but the sum is 0, so there must be another term $\chi(n)$ in the sum such that $\chi(n) \neq 1$, $\chi(n) \neq 0$. But $n \equiv 1 \pmod{d}$, so d is not a quasiperiod of χ, and hence χ is primitive. $\square$

4. Gauss sums

Given a character χ modulo q, we define the Gauss sum $\tau(\chi)$ of χ to be

$$\tau(\chi) = \sum_{a=1}^{q} \chi(a) e(a/q).$$

This may be regarded as the inner product of the multiplicative character $\chi(a)$ with the additive character $e(a/q)$. As such, it is analogous to the gamma function $\Gamma(s) = \int_0^\infty x^{s-1} e^{-x}\, dx$, which is the inner product of the multiplicative character x^s with the additive character e^{-x} with respect to the invariant measure dx/x. Gauss sums are invaluable in transferring questions concerning Dirichlet characters to questions concerning additive characters, and vice versa.

The Gauss sum is a special case of the more general sum

$$c_\chi(n) = \sum_{a=1}^{q} \chi(a) e(an/q).$$

When χ is the principal character, this is Ramanujan's sum

$$c_q(n) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e(an/q),$$

whose properties were discussed in §4.1. We now show that the sum $c_\chi(n)$ is closely related to $\tau(\chi)$.

Theorem 4.1. *Suppose that χ is a character modulo q. If $(n, q) = 1$ then*

$$\chi(n)\tau(\overline{\chi}) = \sum_{a=1}^{q} \overline{\chi}(a) e(an/q), \tag{4.4}$$

and in particular

$$\overline{\tau(\chi)} = \chi(-1)\tau(\overline{\chi}).$$

Proof. If $(n,q) = 1$ then the map $a \mapsto an$ permutes the residues modulo q, and hence

$$\chi(n)c_\chi(n) = \sum_{a=1}^{q} \chi(an)e(an/q) = \tau(\chi).$$

On replacing χ by $\overline{\chi}$, this gives (6), and (7) follows by taking $n = -1$. □

Theorem 4.2. *Suppose that $(q_1, q_2) = 1$, that χ_i is a character modulo q_i for $i = 1, 2$, and that $\chi = \chi_1\chi_2$. Then*

$$\tau(\chi) = \tau(\chi_1)\tau(\chi_2)\chi_1(q_2)\chi_2(q_1).$$

Proof. By the Chinese remainder theorem, each

$$a \pmod{q_1q_2}$$

can be written uniquely as $a_1q_2 + a_2q_1$ with $1 \le a_i \le q_i$. Thus the general term in (3) is

$$\chi_1(a_1q_2)\chi_2(a_2q_1)e(a_1/q_1)e(a_2/q_2),$$

so the result follows. □

For primitive characters the hypothesis that $(n,q) = 1$ in Theorem 5 can be removed.

Theorem 4.3. *Suppose that χ is a primitive character modulo q. Then (4.4) holds for all n, and $|\tau(\chi)| = \sqrt{q}$.*

Proof. It suffices to prove (4.4) when $(n,q) > 1$. Choose m and d so that $(m,d) = 1$ and $m/d = n/q$. Then

$$\sum_{a=1}^{q} \chi(a)e(an/q) = \sum_{h=1}^{d} e(hm/d) \sum_{\substack{a=1 \\ a \equiv h \pmod d}}^{q} \chi(a).$$

Since $d \mid q$ and $d < q$, the inner sum vanishes by Theorem 3.4. Thus (4.4) holds also in this case.

We replace χ in (4.4) by $\overline{\chi}$, take the square of the absolute value of both sides, and sum over n to see that

$$\begin{aligned}\varphi(q)|\tau(\chi)|^2 &= \sum_{n=1}^{q}\left|\sum_{a=1}^{q}\chi(a)e(an/q)\right|^2 \\ &= \sum_{a=1}^{q}\sum_{b=1}^{q}\chi(a)\overline{\chi}(b)\sum_{n=1}^{q}e((a-b)n/q).\end{aligned}$$

The innermost sum on the right is 0 unless $a \equiv b \pmod{q}$, in which case it is equal to q. Thus $\varphi(q)|\tau(\chi)|^2 = \varphi(q)q$, and hence $|\tau(\chi)| = \sqrt{q}$. □

If χ is primitive modulo q then not only does 4.4 hold for all n but also $\tau(\overline{\chi}) \neq 0$, and hence we have

Corollary 4.4. *Suppose that χ is a primitive character modulo q. Then for any integer n,*

$$\chi(n) = \frac{1}{\tau(\overline{\chi})}\sum_{a=1}^{q}\overline{\chi}(a)e(an/q).$$

This is very useful, since it allows us to express the multiplicative character χ as a linear combination of additive characters $e(an/q)$.

We next show that $\tau(\chi)$ can be expressed in terms of $\tau(\chi^\star)$ where $\chi^\star$ is the primitive character that induces χ.

Theorem 4.5. *Let χ be a character modulo q that is induced by the primitive character $\chi^\star$ modulo d. Then $\tau(\chi) = \mu(q/d)\chi^\star(q/d)\tau(\chi^\star)$.*

Proof. If $(d, q/d) > 1$ then $\chi^\star(q/d) = 0$, so we begin by showing that $\tau(\chi) = 0$ in this case. Let p be a prime such that $p \mid d$, $p \mid q/d$, and write $a = jq/p + k$ with $0 \leq j < p$,

$0 \le k < q/p$. Then

$$\tau(\chi) = \sum_{a=0}^{q-1} \chi(a)e(a/q) = \sum_{k=1}^{q/p} \sum_{j=1}^{p} \chi(jq/p + k)e(j/p + k/q).$$

But $p \mid (q/p)$, so $(jq/p + k, q) = 1$ if and only if $(jq/p + k, q/p) = 1$, which in turn is equivalent to $(k, q/p) = 1$. Also, $d \mid q/p$, so the above is

$$= \sum_{\substack{k=1 \\ (k,q/p)=1}}^{q/p} \chi^\star(k)e(k/q) \sum_{j=1}^{p} e(j/p).$$

Here the inner sum vanishes, so $\tau(\chi) = 0$ when $(d, q/d) > 1$.

Now suppose that $(d, q/d) = 1$, and let χ_0 denote the principal character modulo q/d. Then by Theorem 4.2,

$$\tau(\chi) = \tau(\chi_0\chi^\star) = \tau(\chi_0)\tau(\chi^\star)\chi_0(d)\chi^\star(q/d).$$

By taking $n = 1$ in Theorem 4.1 we find that $\tau(\chi_0) = \mu(q/d)$. Thus we have the stated result. □

We now turn our attention to the more general $c_\chi(n)$. To this end we begin with an auxiliary result.

Lemma 4.6. *Let χ be a character modulo q induced by the primitive character $\chi^\star$ modulo d. Suppose that $r \mid q$. Then*

$$\sum_{\substack{n=1 \\ n \equiv b \pmod r}}^{q} \chi(n) = \chi^\star(b)\varphi(q)/\varphi(r)$$

when $(b, r) = 1$ and $d \mid r$, and is 0 otherwise.

Proof. Let $S(b, r)$ denote the sum in question. If $p \mid (b, r)$ and $n \equiv b \pmod r$, then $p \mid n$, and so $(n, q) > 1$. Thus each term in $S(b, r)$ is 0. Thus we are done when $(b, r) > 1$, so we suppose that $(b, r) = 1$. Consider next the case when $d \nmid r$. Then r is not a quasiperiod of χ. Hence there exist m and n such that $(mn, q) = 1$, $m \equiv n \pmod r$, and

$\chi(m) \neq \chi(n)$. Choose c so that $cn \equiv m \pmod q$. Then $c \equiv 1 \pmod r$ and $\chi(c) \neq 1$. Hence $\chi(c)S(b,r) = S(b,r)$, as in the proof of Theorem 4, so $S(b,r) = 0$ in this case. Finally suppose that $d \mid r$. Let χ_0 be the principal character modulo q. If $n \equiv b \pmod r$ then $\chi^\star(n) = \chi^\star(b)$. Thus

$$S(b,r) = \chi^\star(b) \sum_{\substack{n=1 \\ n \equiv b \pmod r}}^{q} \chi_0(n).$$

Write $q/r = q_1 q_2$ where q_1 is the largest divisor of q/r that is relatively prime to r. Then the sum on the right above is

$$\sum_{\substack{k=1 \\ (kr+b, q_1)=1}}^{q_1 q_2} 1 = q_2 \varphi(q_1) = \varphi(q)/\varphi(r),$$

as required. □

We are now in a position to deal with $c_\chi(n)$.

Theorem 4.7. *Let χ be a character modulo q induced by the primitive character $\chi^\star$ modulo d. Put $r = q/(q,n)$. Then $c_\chi(n) = 0$ if $d \nmid r$, while if $d \mid r$ then*

$$c_\chi(n) = \overline{\chi}^\star(n/(q,n))\chi^\star(r/d)\mu(r/d)\frac{\varphi(q)}{\varphi(r)}\tau(\chi^\star).$$

Proof. If $(n,q) = 1$ then by (4.4) and Theorem 4.5 we see that

$$c_\chi(n) = \overline{\chi}(n)\tau(\chi) = \overline{\chi}^\star(n)\mu(q/d)\chi^\star(q/d)\tau(\chi^\star).$$

Since $r = q$, we have $d \mid r$, so we have the correct result. Now suppose that $(n,q) > 1$. In the definition (4) of $c_\chi(n)$, let $a = br + k$ with $0 \leq b < q/r$, $1 \leq k \leq r$. Then

$$c_\chi(n) = \sum_{k=1}^{r} e(kn/q) \sum_{b=1}^{q/r} \chi(br + k).$$

By Lemma 4.6 this is 0 when $d \nmid r$. Thus we may suppose that $d \mid r$. Then, by Lemma 4.6,

$$c_\chi(n) = \sum_{\substack{k=1 \\ (k,r)=1}}^{r} e(kn/q)\chi^\star(k)\varphi(q)/\varphi(r).$$

Put $m = n/(q,n)$, and let χ_1 denote the character modulo r induced by $\chi^\star$. Then the above is

$$= \frac{\varphi(q)}{\varphi(r)} \sum_{k=1}^{r} e(km/r)\chi_1(k).$$

Since $(m,r) = 1$, we see by the first case treated that the above is

$$\frac{\varphi(q)}{\varphi(r)}\overline{\chi}^\star(m)\mu(r/d)\chi^\star(r/d)\tau(\chi^\star),$$

which suffices. □