DIRICHLET'S THEOREM ON PRIMES IN PROGRESSIONS, III

K. Soundararajan

In the preceding two articles we obtained Dirichlet's theorem for progressions with common difference 3, 4, 5, and 8. Now we aim to generalize the ideas behind those proofs for an arbitrary modulus q. One of the main ideas in our previous proofs was to define periodic multiplicative functions such that every reduced residue class under consideration could be expressed as a linear combination of these functions. Our immediate goal is to describe the general theory of such functions. For a general modulus q there are $\phi(q)$ reduced residue classes, and accordingly we are looking for $\phi(q)$ multiplicative functions with period q.

The functions that we seek are known as *Dirichlet characters*, and we now give a precise definition for this term. A function $\chi : \mathbb{Z} \to \mathbb{C}$ is called a Dirichlet character $\pmod q$ if it satisfies the following criteria:

(i) $\chi(n)$ is not always zero;

(ii) $\chi(n) = 0$ if $(n, q) > 1$;

(iii) χ is periodic with period q: that is $\chi(n + q) = \chi(n)$ for all n;

(iv) χ is (completely) multiplicative[1]: that is $\chi(mn) = \chi(m)\chi(n)$ for all integers m and n.

Sometimes we shall just call a Dirichlet character as a character, or write $\chi \pmod q$ to indicate that it's a character with modulus (or period) q.

Let us now record some immediate consequences of this definition. For any integer n we have $\chi(n) = \chi(n \cdot 1) = \chi(n)\chi(1)$ by (iv), and since $\chi(n) \neq 0$ for some n by (i), we conclude that $\chi(1) = 1$. Next if $(n, q) = 1$ then, using (iv, iii) and Euler's theorem that $n^{\phi(q)} \equiv 1 \pmod q$

$$\chi(n)^{\phi(q)} = \chi(n^{\phi(q)}) = \chi(1) = 1,$$

so that $\chi(n)$ is a $\phi(q)$-th root of unity. This observation also means that there are only finitely many characters; to describe a character we need only give its values on the reduced residue classes $\pmod q$ and as we've just noted there are only $\phi(q)$ possible values that can be taken by any reduced residue class.

We also note that there is always at least one Dirichlet character $\pmod q$: this is the principal (or trivial character) defined by setting

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

[1] A function which satisfies $f(mn) = f(m)f(n)$ for coprime integers m and n is said to be multiplicative. A completely multiplicative function satisfies $f(mn) = f(m)f(n)$ for all integers m and n.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

If χ and ψ are two characters $\pmod q$ then we may define a character $\chi\psi \pmod q$ by setting

$$\chi\psi(n) = \chi(n)\psi(n).$$

It is a simple matter, left to you, to check that this is indeed a character.

Proposition 1. *Let $\mathcal{G}$ denote the set of Dirichlet characters $\pmod q$. Under the operation of multiplying two characters given above, $\mathcal{G}$ forms a finite abelian group. The identity element of this group is the principal character χ_0. The inverse of a character χ is the complex conjugate character $\overline{\chi}$ defined by $\overline{\chi}(n) = \overline{\chi(n)}$.*

Proof. These are all easy statements, and you should have little difficulty in checking them.

Our goal is to describe this group of characters $\mathcal{G}$. Let us start with the case when q is the power of an odd prime p.

Proposition 2. *If $q = p^\alpha$ is the power of an odd prime p then there are exactly $\phi(q)$ characters $\pmod q$, and the group $\mathcal{G}$ is cyclic.*

Proof. Recall that there is a primitive root $\pmod q$; say g. Any character $\chi \pmod q$ is determined by its value on g, since all the reduced residue classes $\pmod q$ are just some powers of g. Moreover $\chi(g)$ must be some $\phi(q)$-th root of unity. Thus we must have $\chi(g) = e^{2\pi i a/\phi(q)}$ where $a = 0, 1, \ldots, \phi(q) - 1$, and each choice of this root of unity leads to a (distinct) character. Note that χ_0 arises from the choice $a = 0$; check that every character is a power of the character obtained by setting $a = 1$.

We can also determine what happens when $q = 2^\alpha$. When $\alpha = 1$ there is nothing to do, $\alpha = 2$ and 3 we have handled before (check that there are no other ways of getting characters), and consider now $\alpha \ge 3$. Recall that every element of $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ can be written as $\pm 5^k$ where $k = 1, \ldots, 2^{\alpha-2}$. Thus we only have to define $\chi(-1)$ and $\chi(5)$. The only choices for $\chi(-1)$ are ± 1, and $\chi(5)$ has to be some $2^{\alpha-2}$-th root of unity. This describes a way to get $\phi(2^\alpha)$ different characters, and these are all.

Proposition 3. *(Orthogonality Relation 1) Let q be any natural number, and let $\chi \pmod q$ be a Dirichlet character. Then*

$$\sum_{n \pmod q} \chi(n) = \begin{cases} \phi(q) & \text{if } \chi = \chi_0 \\ 0 & \text{if not.} \end{cases}$$

If χ and ψ are two characters $\pmod q$ then

$$\sum_{n \pmod q} \chi(n)\overline{\psi}(n) = \begin{cases} \phi(q) & \text{if } \chi = \psi \\ 0 & \text{if not.} \end{cases}$$

Proof. Using the first assertion for the character $\chi\overline{\psi}$ we immediately obtain the second assertion of our Proposition. So we only need to prove the first statement. Call the sum in question $S(\chi)$. Let c be any integer coprime to q. Then

$$\chi(c)S(\chi) = \sum_{n \pmod q} \chi(c)\chi(n) = \sum_{n \pmod q} \chi(cn).$$

Now, as n ranges over all the residue classes $\pmod q$, so does $m = cn$. Therefore the above equals

$$\sum_{m \pmod q} \chi(m) = S(\chi).$$

We conclude that

$$S(\chi)\chi(c) = S(\chi),$$

so that either $S(\chi) = 0$, or $\chi(c) = 1$. Since c was an arbitrary reduced residue class $\pmod q$, either we must have $S(\chi) = 0$ or $\chi(c) = 1$ for all reduced residue classes $c \pmod q$. The latter statement simply means that $\chi = \chi_0$. So either $S(\chi) = 0$ or $\chi = \chi_0$, and it is easy to see that $S(\chi_0) = \phi(q)$.

So far we have described completely what the $\phi(p^\alpha)$ characters $\pmod{p^\alpha}$ are. It remains now to describe the characters $\pmod q$ for arbitrary composite numbers q. First we shall describe a means of constructing $\phi(q)$ characters $\chi \pmod q$, and then we shall show that there are no other possible characters.

Let $q = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ where the primes $p_1, \ldots, p_k$ are distinct. Given characters $\chi_1 \pmod{p_1^{\alpha_1}}$, $\chi_2 \pmod{p_2^{\alpha_2}}$, $\ldots$, $\chi_k \pmod{p_k^{\alpha_k}}$, we may construct a character $\chi \pmod q$ by defining $\chi(n) = \chi_1(n)\chi_2(n)\cdots\chi_k(n)$; you should check that χ is indeed a character $\pmod q$. Further let us note that if $\psi_1 \pmod{p_1^{\alpha_1}}$, $\ldots$, $\psi_k \pmod{p_k^{\alpha_k}}$ are some other characters with say $\psi_1 \neq \chi_1$ then the resulting character $\psi \pmod q$ is different from χ. To see this choose $c \pmod{p_1^{\alpha_1}}$ with $\chi_1(c) \neq \psi_1(c)$ and pick $n \pmod q$ such that $n \equiv c \pmod{p_1^{\alpha_1}}$ and $n \equiv 1 \pmod{q/p_1^{\alpha_1}}$. Then $\chi(n) = \chi_1(c) \neq \psi_1(c) = \psi(n)$ and so the characters χ and ψ are distinct as claimed. Thus by this device we have constructed $\phi(p_1^{\alpha_1})\cdots\phi(p_k^{\alpha_k}) = \phi(q)$ different characters $\chi \pmod q$.

The $\phi(q)$ characters described above form a group (check). Call this group $\mathcal{H}$ which is thus a subgroup of $\mathcal{G}$ and we claim that in fact $\mathcal{G} = \mathcal{H}$; that is, there are no other characters. Postponing the last assertion for the moment, let us prove a variant (and for us the more useful) of the orthogonality relation established above.

Proposition 4. *(Orthogonality Relation 2) Let $a \pmod q$ be a reduced residue class. Then*

$$\sum_{\chi \in \mathcal{H}} \chi(n)\overline{\chi}(a) = \begin{cases} \phi(q) & \text{if } n \equiv a \pmod q \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Note that if a^{-1} denotes the multiplicative inverse of $a \pmod q$ (thus $aa^{-1} \equiv 1 \pmod q$) then $\chi(a^{-1}) = 1/\chi(a) = \overline{\chi}(a)$. Therefore our desired sum may be written as

$$S(na^{-1}) := \sum_{\chi \in \mathcal{H}} \chi(na^{-1}).$$

Now let ψ be a character in $\mathcal{H}$ and note that as χ varies over all the characters in $\mathcal{H}$ then so does $\psi\chi$. Therefore

$$\psi(na^{-1})S(na^{-1}) = \sum_{\chi \in \mathcal{H}} \psi\chi(na^{-1}) = \sum_{\chi \in \mathcal{H}} \chi(na^{-1}) = S(na^{-1}).$$

Therefore either $S(na^{-1}) = 0$ or $\psi(na^{-1}) = 1$.

If $S(na^{-1}) \neq 0$ then from the above it follows that $\psi(na^{-1}) = 1$ for all the characters $\psi \in \mathcal{H}$, but this readily implies that $na^{-1} \equiv 1 \pmod q$ (why?) and so $n \equiv a \pmod q$. Finally, if $n \equiv a \pmod q$ then our sum is clearly $\phi(q)$. Thus the Proposition has been established.

Proposition 5. *The group of characters $\mathcal{G}$ equals the group of characters $\mathcal{H}$ that we have constructed explicitly.*

Proof. Suppose to the contrary that X is some character in $\mathcal{G}$ which is not in $\mathcal{H}$. Then for any $\chi \in \mathcal{H}$ we have that $X\overline{\chi} \in \mathcal{G}$ is not the principal character, and this means by Proposition 3 that

$$\sum_{n \pmod q} X(n)\overline{\chi}(n) = 0.$$

Multiply both sides by $\chi(c)$ for some $(c,q) = 1$, and sum over all $\chi \in \mathcal{H}$. Then

$$0 = \sum_{\chi \in \mathcal{H}} \chi(c) \sum_{n \pmod q} X(n)\overline{\chi}(n) = \sum_{n \pmod q} X(n) \sum_{\chi \in \mathcal{H}} \chi(c)\overline{\chi}(n) = \phi(q)X(c),$$

upon using Proposition 4 in the final step above. Therefore $X(c) = 0$, and since c was arbitrary, we conclude that $X(c) = 0$ for all c, which is nonsense. So $\mathcal{G} = \mathcal{H}$ and we have described all the Dirichlet characters $\pmod q$ explicitly.

Now that we know what all the characters $\pmod q$ are, we may write Proposition 4 as saying, for $(a,q) = 1$,

$$\frac{1}{\phi(q)} \sum_{\chi \pmod q} \chi(n)\overline{\chi}(a) = \begin{cases} 1 & \text{if } n \equiv a \pmod q \\ 0 & \text{otherwise.} \end{cases}$$

This relation generalizes all our examples for $q = 3$, 4, 5, 8 where we were able to express the different reduced residues in terms of characters; now we know the general pattern!

Back then to Dirichlet's theorem. Corresponding to every character $\chi \pmod q$ we define

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

This converges absolutely for $s > 1$. Moreover as before we have

$$\log L(s,\chi) = \sum_p \frac{\chi(p)}{p^s} + O(1).$$

Now given a reduced residue class $a \pmod q$, from our orthogonality relations we have

$$\sum_{p \equiv a \pmod q} \frac{1}{p^s} = \frac{1}{\phi(q)} \sum_{\chi \pmod q} \overline{\chi}(a) \sum_p \frac{\chi(p)}{p^s} = \frac{1}{\phi(q)} \sum_{\chi \pmod q} \overline{\chi(a)} \log L(s,\chi) + O(1).$$

The term $\chi = \chi_0$ above contributes

$$\frac{\overline{\chi_0(a)}}{\phi(q)} \log L(s, \chi_0) = \frac{1}{\phi(q)} \log \frac{1}{s-1} + O(1),$$

since $L(s, \chi_0) = \zeta(s) \prod_{p|q}(1 - 1/p^s)$. Thus in order to show that $\sum_{p \equiv a \pmod q} p^{-s}$ diverges as $s \to 1^+$ we need only show that as $s \to 1$ and for $\chi \neq \chi_0$ we have $L(s, \chi)$ tends neither to zero nor to infinity. This will ensure that the terms $\log L(s, \chi)$ for $\chi \neq \chi_0$ will remain bounded as $s \to 1^+$ and that would complete our proof. We shall deal with this problem in our next set of notes.