Miniproject - Analytic Number Theory

Simon Pohmann

We use the convention that $\mathbb{N} = \{n \in \mathbb{Z} \mid n \geq 0\}$. Further, we write $a \mid b$ if a divides b and $a \perp b$ if a and b are coprime. Finally, let $\mathbb{P}$ be the set of prime numbers in $\mathbb{N}$.

1 Part I

For convenience, we include the definition of a Dirichlet character from the task description first.

Definition 1. Let $q \geq 2$, then a *Dirichlet character (mod q)* is a function $\chi : \mathbb{N} \to \mathbb{C}$ such that

- χ is completely multiplicative, so $\chi(a)\chi(b) = \chi(ab)$
- χ is periodic modulo q, so $\chi(n + q) = \chi(n)$
- $\chi(n) \neq 0$ if and only if $n \perp q$

First, we will give another characterization of Dirichlet characters.

Lemma 2 (Characterization of Dirichlet characters)**.** We have a one-to-one correspondence between Dirichlet characters mod q and group homomorphisms $(\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$ via

$$\begin{aligned}\{f : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times \mid f \text{ group hom}\} &\to \{\chi : \mathbb{N} \to \mathbb{C} \mid \chi \text{ Dirichlet character mod } q\} \\ f &\mapsto \chi_f := \left(\mathbb{N} \to \mathbb{C},\ n \mapsto \begin{cases} f([n]) & \text{if } n \perp q \\ 0 & \text{otherwise} \end{cases}\right)\end{aligned}$$

Proof. First of all, we show that the map is well-defined. Let $f : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$ be a (multiplicative) group homomorphism, and we show that χ_f is a Dirichlet character.

Note that property (ii) and (iii) directly follow from the definition, as $\chi_f(n)$ only depends on the value of $n \mod q$. So consider some $a, b \in \mathbb{N}$. If both $a \perp q$ and $b \perp q$ then

$$\chi_f(a)\chi_f(b) = \chi([a])\chi([b]) = \chi([ab]) = \chi_f(ab)$$

as also $ab \perp q$.

On the other hand, if $a \not\perp q$ or $b \not\perp q$ have $\chi_f(a) = 0$ resp. $\chi_f(b) = 0$. We also have in this case that $ab \not\perp q$ and so

$$\chi_f(a)\chi_f(b) = 0 = \chi_f(ab)$$

Now it is left to show that the correspondence is a bijection. Clearly, if $f \neq g$ then $f(x) \neq g(x)$ for some $x \in (\mathbb{Z}/q\mathbb{Z})^\times$ and so $\chi_f(n) \neq \chi_g(n)$ for some representative $n \in \mathbb{N}$ of x.

To show surjectivity, consider some Dirichlet character $\chi : \mathbb{N} \to \mathbb{C}$ and construct a group homomorphism $f : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$. For each $x \in (\mathbb{Z}/q\mathbb{Z})^\times$, there is a representative $n \in \mathbb{N}$ of x and as $\chi(n)$ does not depend on the choice of n, we may define $f(x) := \chi(n)$. Note that as $x \in (\mathbb{Z}/q\mathbb{Z})^\times$, we find $n \perp q$ and so $\chi(n) \neq 0$, i.e. $\chi(n) \in \mathbb{C}^*$. Then clearly for $a, b \in (\mathbb{Z}/q\mathbb{Z})^*$ with representatives $n, m \in \mathbb{N}$ have

$$f(ab) = \chi(nm) = \chi(n)\chi(m) = f(a)f(b)$$

So f is a well-defined group homomorphism and we obviously have $\chi_f = \chi$. $\square$

For simplicity of notation we sometimes will identify a Dirichlet character and its group homomorphism if it is always clear which one is meant.

Example 3 (Ex (i))**.** The function

$$f : \mathbb{N} \to \mathbb{C}, \quad n \mapsto \begin{cases} 0 & \text{if } n \equiv 0, 2 \mod 4 \\ 1 & \text{if } n \equiv 1 \mod 4 \\ -1 & \text{if } n \equiv 3 \mod 4 \end{cases}$$

is a Dirichlet character.

Proof. This follows directly from Lemma 2, as $f = \chi_g$ for the group homomorphism

$$g : (\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\} \to \mathbb{C}^*, \quad 1 \mapsto 1,\ 3 \mapsto -1$$

(this is a group homomorphism, as $3^2 = 9 \equiv 1 \mod 4$) $\square$

Now we want to define Dirichlet series of Dirichlet characters.

Proposition 4. For a Dirichlet character $\chi : \mathbb{N} \to \mathbb{C}$ and some $\epsilon > 0$, the series

$$L(s, f) := \sum_{n \geq 1} f(n) n^{-s}$$

converges uniformly on $\Re(s) \geq 1 + \epsilon$. We will call it the Dirichlet series of χ.

Proof. By Lemma 2, we know that χ corresponds to a group homomorphism $f : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$ such that $\chi(\mathbb{N}) = f((\mathbb{Z}/q\mathbb{Z})^*) \cup \{0\} \subseteq \mathbb{C}$ is a finite subset of $\mathbb{C}$. Hence, there is $C > 0$ with $|\chi(n)| \leq C$ for all $n \in \mathbb{N}$, and it follows that

$$\sum_{1 \leq n \leq X} \left|\chi(n) n^{-s}\right| \leq \sum_{1 \leq n \leq X} C \left|n^{-s}\right| \leq C \sum_{1 \leq n \leq X} n^{-1-\epsilon} \leq C \sum_{n \geq 1} n^{-1-\epsilon}$$

which is finite. $\square$

Proposition 5. Let $f : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$ be a group homomorphism. Then for the associated Dirichlet character $\chi = \chi_f$ we have that

$$\lim_{s\to 1^+} L(s,\chi) \text{ exists } \Leftrightarrow \sum_{x\in(\mathbb{Z}/q\mathbb{Z})^\times} f(x) = 0$$

In this case, have that $L(s,\chi)$ is well-defined, $\lim_{t\to s} L(t,\chi)$ exists and

$$\lim_{t\to s} L(t,\chi) = \sum_{n\geq 1} \chi(n) n^{-s}$$

where the right sum converges (but not absolutely), for all $\Re(s) > 0$.

Proof. Let $c = \sum_{x\in(\mathbb{Z}/q\mathbb{Z})^\times} f(x)$. For the direction $\Rightarrow$ assume that $c \neq 0$. Then have for $\Re(s) > 1$ that

$$\begin{aligned}
\operatorname{sgn}(c)\sum_{n\geq 1}\chi(n)n^{-s} &= \sum_{n\geq 1}\sum_{0\leq k<q} \operatorname{sgn}(c)\chi(qn+k)(qn+k)^{-s} \\
&\geq \sum_{n\geq 1}\sum_{0\leq k<1} \operatorname{sgn}(c)\chi(qn+k)(qn+n)^{-s} \\
&= \sum_{n\geq 1} \operatorname{sgn}(c)(qn+n)^{-s} \underbrace{\sum_{0\leq k<q}\chi(qn+k)}_{=c} \\
&\geq \frac{|c|}{(q+1)^s}\sum_{n\geq 1} n^{-s} = \frac{|c|}{(q+1)^s}\zeta(s)
\end{aligned}$$

which clearly has a pole at $s = 1$. Hence $\lim_{s\to 1^+} L(s,\chi_f)$ cannot exist.

For the other direction, assume that $c = 0$. Again, have for $\Re(s) > 1$ that

$$\begin{aligned}
\sum_{n\geq 1}\chi(n)n^{-s} &= \sum_{n\geq 1}\sum_{0\leq k<q}\chi(qn+k)(qn+k)^{-s} \\
&= \sum_{n\geq 1}\sum_{0\leq k<q}\chi(qn+k)\Big((qn)^{-s} + (qn+k)^{-s} - (qn)^{-s}\Big)
\end{aligned}$$

Observe that by Bernoulli's inequality, have

$$\begin{aligned}
(qn)^{-s} - (qn+k)^{-s} &= \frac{(qn)^s - (qn+k)^s}{(q^2n^2+qnk)^s} = (qn)^s\frac{1-(1+k(qn)^{-1})^s}{(q^2n^2+qnk)^s} \\
&\leq (qn)^s\frac{sk(qn)^{-1}}{(q^2n^2+qnk)^s} = \frac{sk}{qn(qn+k)^s} = O(sn^{-s-1})
\end{aligned}$$

As $\chi((\mathbb{Z}/q\mathbb{Z})^\times) \subseteq \mathbb{C}$ is finite, find $C > 0$ with $|\chi_f(n)| \leq C$ for all $n \in \mathbb{N}$. Then

$$\begin{aligned}\sum_{n\geq X} \chi(n)n^{-s} = O(qCX^{-s}) + \sum_{n\geq X/q} \sum_{0\leq k<q} \chi(qn+k)\Big((qn)^{-s} + O(sn^{-s-1})\Big) \\ = O(qCX^{-s}) + \sum_{n\leq X/q} \Big((qn)^{-s}c + \sum_{0\geq k<q} O(Csn^{-s-1})\Big) = \\ = O(qCX^{-s}) + 0 + O\Big(Cqs \sum_{n\geq X/q} n^{-s-1}\Big) \\ \leq O(qCX^{-s}) + O\Big(Cqs\zeta(s+1)\Big)\end{aligned}$$

which is well-defined and finite for $\Re(s) > 0$. Further, the expression converges uniformly (as a function in s on $\Re(s) \geq \epsilon > 0$) to 0 as $X \to \infty$. So

$$\sum_{n<X} \chi(n)n^{-s} \quad \text{converges uniformly to} \quad \sum_{n\geq 1} \chi(n)n^{-s}$$

as $X \to \infty$ (on a $\Re(s) \geq \epsilon > 0$). Thus the limit is continuous and a continuation of $L(s, \chi_f)$ defined on $\Re(s) > 1$. From this it follows that $\lim_{t\to s} L(t, \chi_f)$ exists and is equal to $\sum_n \chi_f(n)n^{-s}$. □

Applied to our example, we find

Example 6 (Ex (ii))**.** Let $f : \mathbb{N} \to \mathbb{C}$ be the Dirichlet character from Example 3 with corresponding group homomorphism $g : (\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{C}$. Then

$$\sum_{x\in(\mathbb{Z}/4\mathbb{Z})^*} g(x) = g(1) + g(3) = 1 - 1 = 0$$

and so by Lemma 5 the limit $\lim_{s\to 1^+} L(s, f)$ exists. The lemma further yields that

$$\begin{aligned}\lim_{s\to 1} L(s, f) = \sum_{n\geq 1} f(n)n^{-1} = \sum_{n\geq 0} \frac{f(4n+1)}{4n+1} + \frac{f(4n+3)}{4n+3} = \sum_{n\geq 0} \frac{1}{4n+1} - \frac{1}{4n+3} \\ = 2\sum_{n\geq 0} \frac{1}{(4n+1)(4n+3)} > 0\end{aligned}$$

is positive. Wolfram Alpha [Wol] can give an explicit value to this sum, using the digamma function ψ. Namely

$$\sum_{x\in(\mathbb{Z}/4\mathbb{Z})^\times} f(n)n^{-1} = \frac{1}{4}(\psi(\frac{7}{4}) - \psi(\frac{5}{4}))$$

which seems to be $\frac{1}{4}$.

Now we want to study the series

$$\sum_p f(p)p^{-s}$$

For this, we are first interested in how many primes $\equiv 1, 3 \mod 4$ there are.

Lemma 7. Let $n \equiv 3 \mod 4$. Then n has a prime factor $p \equiv 3 \mod 4$.

Proof. Use induction on n. If $n = 3$, the claim is trivial. So let $n > 3$. If n is prime, the claim again follows. Otherwise, have $n = ab$ with nontrivial divisors a, b. However, $3 \equiv n$ is not a square modulo 4, so find that $a \not\equiv b \mod 4$. As both a and b must be odd, we see that either $a \equiv 3 \mod 4$ or $b \equiv 3 \mod 4$ and the claim follows by the induction hypothesis. □

Corollary 8 (Ex (iii))**.** There are infinitely many primes p with $p \equiv 3 \mod 4$.

Proof. Assume there were only finitely many, say $p_1, ..., p_N$. Let $P := p_1...p_N$ if N is even and $P := p_1^2 p_2...p_N$ if N is odd. Then

$$P \equiv 3^{2\lceil \frac{N}{2} \rceil} \equiv 1^{\lceil \frac{N}{2} \rceil} = 1 \mod 4$$

Thus, by Lemma 7, $P+2$ has a prime factor $q \equiv 3 \mod 4$. However, $q \neq p_i$ as $p_i \perp P+2$ for all i (if $p_i \mid P+2$, then $p_i \mid P+2-P = 2$, a contradiction). This contradicts our assumption. □

For the case of primes $\equiv 1 \mod 4$, I have remembered the two-square theorem and its connection to primes in the ring $\mathbb{Z}[i]$ of Gaussian integers, and somehow my train of thoughts went into Algebraic Number Theory. After some research, I have found an exercise in [Neu92, Chapter I, §10] that requires the reader to prove the following proposition.

Proposition 9. Let $q \geq 3$ be an integer. Then there are infinitely many primes p with $p \equiv 1 \mod q$.

Proof. Assume there were only finitely many such primes p_i, then we have their product $P = \prod_i p_i \in \mathbb{Z}$. Consider now the q-th cyclotomic polynomial Φ_q. Clearly $\Phi_q(qPX) - 1 \in \mathbb{Q}[X]$ has at most $\phi(q)$ zeros, so there exists some $x \in \mathbb{Z}$ with $\Phi_q(qPx) \neq 1$ (this "Ansatz" was given as a hint).

Let now $K = \mathbb{Q}(\omega_q)$ be the q-th cyclotomic number field with a primitive q-th root of unity ω_q (i.e. $\Phi_q(\omega_q) = 0$). Let further $\mathcal{O} \subseteq K$ be the ring of integral elements over $\mathbb{Z}$ in K. The prime decomposition law for Dedekind ring extension [Neu92, Chapter I, Prop 8.3] tells us that for a prime p, the ideal (p) is reducible in $\mathcal{O}$ if and only if $\Phi_q \mod p$ is reducible. As $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$, this is the case if and only if $q \mid p-1$, i.e. $p \equiv 1 \mod q$.

Now consider the element $\alpha = \omega_q - xqP \in \mathcal{O}$. Then

$$\begin{aligned} N_{K/\mathbb{Q}}(\alpha) &= \prod_{\sigma:K\to\mathbb{C}\ \mathbb{Q}\text{-field homomorphism}} \sigma(\omega_q - xqP) \\ &= \prod_{\sigma} (\sigma(\omega_q) - xqP) = \mathrm{MiPo}_{\mathbb{Q}}(\omega_q)(xqP) = \Phi_q(xqP) \neq 1 \end{aligned}$$

as $\mathrm{MiPo}_{\mathbb{Q}}(\omega_q) = \prod_\sigma(\sigma(\omega_q) - X)$. Hence, α is not a unit in $\mathcal{O}$. On the other hand, (α) is coprime to (p_i) for each p_i, as

$$\omega_q = \alpha - xqP \in (\alpha) + (p_i) \quad \text{and} \quad \omega_q \in \mathcal{O}^\times$$

By our assumption, the only prime ideals in $\mathcal{O}$ are the prime ideal factors of (p_i) and (p) for $p \neq p_i$. Thus, the prime ideal factorization of (α) consists only of prime ideals $(p), p \neq p_i$ and it follows that $(\alpha) = (n)$ for some integer $n \geq 2$. As ω_q and $xqP \in \mathbb{Z}$ are $\mathbb{Q}$-linearly independent, we see that $n \mid \omega_q$ and $n \mid xqP$. However, the former is a contradiction, as $\omega_q \in \mathcal{O}^\times$ is a unit and no $n \geq 2$ is a unit. □

The book also mentions that the general case can be proven by using L-series in algebraic number fields.

Corollary 10 (Ex (iii))**.** There are infinitely many primes p with $p \equiv 1 \mod 4$.

Proof. This is just a special case of Prop. 9. □

Example 11 (Ex (iii))**.** Using a computer, we can also study the actual frequency of prime numbers $\equiv 1, 3 \mod 4$ among e.g. the first 10^8 integers. This seems to indicate that both numbers are asymptotically equal. For example, there are 332180 primes $\equiv 1 \mod 4$ and 332398 primes $\equiv 3 \mod 4$ smaller than 10^8. To find these numbers, the following python code was used.

```python
import itertools
import math

def primes():
    yield 2
    found_primes = [2]
    for n in itertools.count(3):
        for p in found_primes:
            if n % p == 0:
                break
            elif p >= math.sqrt(n):
                yield n
                found_primes.append(n)
                break

def primes_leq(n):
```

```
    return itertools.takewhile(lambda p: p <= n, primes())

for i in range(1, 8):
    print("Consider interval [1, 10**" + str(i) + "]")
    print("  Number of primes = 1 mod 4 is " + str(
        sum(1 for p in primes_leq(10**i) if (p - 1) % 4 == 0)
    ))
    print("  Number of primes = 3 mod 4 is " + str(
        sum(1 for p in primes_leq(10**i) if (p - 3) % 4 == 0)
    ))
    print()
```

2 Part II

We have already shown that Dirichlet characters are, in principle, group homomorphisms $(\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$. If we now assume q to be prime, we get an even nicer characterization.

Corollary 12 (Ex (i))**.** Let $\chi, \chi' : \mathbb{N} \to \mathbb{C}$ be Dirichlet characters mod q and r a representative of a primitive root modulo q. If $\chi(r) = \chi'(r)$, then $\chi = \chi'$. Further, have that $\chi(n)^{q-1} = 1$ for all $n \in \mathbb{N}$ with $n \perp q$.

Proof. The properties follow directly from Lemma 2. Let $f, f' : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$ be the associated group homomorphisms of χ, χ' as in Lemma 2. If $f([r]) = \chi(r) = \chi'(r) = f'([r])$ then clearly $f = f'$, as these are group homomorphisms and $\langle [r] \rangle = (\mathbb{Z}/q\mathbb{Z})^\times$. Hence $\chi = \chi'$.

Further, have for $n \in \mathbb{N}$ with $n \perp q$ that $[n] \in (\mathbb{Z}/q\mathbb{Z})^\times$ and thus

$$[n]^{q-1} = [n]^{\phi(q)} = [n]^{|(\mathbb{Z}/q\mathbb{Z})^\times|} = 1$$

As f is a group homomorphism, find

$$\chi(n)^{q-1} = f([n])^{q-1} = f([n]^{q-1}) = f(1) = 1$$

□

This correspondence also works in the other direction.

Corollary 13 (Ex (ii))**.** Let $\omega \in \mathbb{C}$ be a $(q-1)$-th root of unity, i.e. $\omega^{q-1} = 1$ and let $r \in \mathbb{Z}$ be a representative of a primitive root modulo q. Then

$$g : \mathbb{N} \to \mathbb{C}, \quad n \mapsto \begin{cases} \omega^{\log_r n} & \text{if } n \perp q \\ 0 & \text{otherwise} \end{cases}$$

is a well-defined Dirichlet character.

Proof. Follows again directly from Lemma 2, as $[r] \mapsto \omega$ induces a unique group homomorphism $(\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$. The associated Dirichlet character is obviously g. □

Note that the image of a group homomorphism $f : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$ is a subgroup of $\mathbb{C}^\times$. Using Corollary 12, we can describe it quite concretely.

Proposition 14. Let $\chi : \mathbb{N} \to \mathbb{C}$ be a Dirichlet character with group homomorphism $f : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$. Then $\mathrm{im} f \leq S$ is a subgroup where $S_q := \{\omega_q^k \mid k \in \mathbb{Z}\}$ is the group of q-th roots of unity.

It is a fact from Algebra that $S_q \cong (\mathbb{Z}/q\mathbb{Z})^\times$, hence Dirichlet characters modulo a prime q are in 1-to-1 correspondence with the endomorphisms $\mathrm{End}((\mathbb{Z}/q\mathbb{Z})^\times)$ of $(\mathbb{Z}/q\mathbb{Z})^\times$.

Proof. We have that $S_q = \{x \in \mathbb{C}^\times \mid x^{q-1} = 1\}$ and the claim directly follows from Corollary 12. □

Note that the endomorphism monoid $\mathrm{End}((\mathbb{Z}/q\mathbb{Z})^\times)$ is not a group, except in the trivial case $q = 2$. The reason is that e.g. the trivial group homomorphism $r \mapsto 1$ is not surjective and thus not invertible.

Definition 15. Denote by $\mathrm{Dir}(q)$ the set of Dirichlet characters modulo q.

By Corollary 13 each group endomorphism $f \in \mathrm{End}((\mathbb{Z}/q\mathbb{Z})^\times)$ is determined by its value at a primitive root of unity $r \in (\mathbb{Z}/q\mathbb{Z})^\times$, hence

$$|\mathrm{Dir}(q)| = |\mathrm{End}((\mathbb{Z}/q\mathbb{Z})^\times)| = |(\mathbb{Z}/q\mathbb{Z})^\times| = q - 1$$

It follows that there are exactly $q - 1$ distinct Dirichlet characters modulo a prime q.

Remark 16. It is again a fact that $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is cyclic for an odd prime p and $k \geq 1$. Hence, everything up to now can also be done for odd prime powers, if we replace $q - 1$ by $\phi(q)$.

Because of Lemma 5 it might seem like a good idea to study in which cases the value $\sum_{x \in (\mathbb{Z}/q\mathbb{Z})^\times} \chi(x)$ is zero.

Proposition 17 (Ex (iii))**.** Let χ_0 be the trivial Dirichlet character given by $r \mapsto 1$. Then

$$\sum_{a \in (\mathbb{Z}/q\mathbb{Z})^\times} \chi(a) = \begin{cases} q-1 & \text{if } \chi = \chi_0 \\ 0 & \text{otherwise} \end{cases},$$

$$\sum_{\chi \in \mathrm{Dir}(q)} \chi(a) = \begin{cases} q-1 & \text{if } a \equiv 1 \mod q \\ 0 & \text{otherwise} \end{cases}$$

Furthermore, for $b \perp q$ have

$$\sum_{\chi \in \mathrm{Dir}(q)} \chi(a)\overline{\chi(b)} = \begin{cases} q-1 & \text{if } a \equiv b \mod q \\ 0 & \text{otherwise} \end{cases}$$

Proof. Clearly

$$\sum_{a \in (\mathbb{Z}/q\mathbb{Z})^\times} \chi_0(a) = q - 1 \quad \text{and} \quad \sum_{\chi \in \mathrm{Dir}(q)} \chi(1) = \sum_{\chi \in \mathrm{Dir}(q)} 1 = q - 1$$

So it is left to show that we get zero in the other cases.

Consider a Dirichlet character $\chi \neq \chi_0$ given by $r \mapsto \xi$ for a q-th root of unity $\xi \neq 1$. Then

$$\sum_{a \in (\mathbb{Z}/q\mathbb{Z})^\times} \chi(a) = \sum_{k=0}^{q-2} \chi(r^k) = \sum_{k=0}^{q-2} \xi^k = \frac{1 - \xi^{q-1}}{q - \xi} = 0$$

By using the earlier results on the structure of $\mathrm{Dir}(q)$ we see that for $a = r^k \not\equiv 1 \mod q$, have

$$\begin{aligned} \sum_{\chi \in \mathrm{Dir}(q)} \chi(a) &= \sum_{\chi \in \mathrm{Dir}(q)} \chi(r)^k \\ &= \sum_{\xi\ q\text{-th root of unity}} \xi^k = \sum_{l=0}^{q-2} \omega^{kl} = \frac{1 - (\omega^{q-1})^k}{1 - \omega^k} = 0 \end{aligned}$$

where ω is a primitive q-th root of unity.

For the last part, note that for any q-th root of unity ξ, we have $\xi\overline{\xi} \in \mathbb{R}$ with $\xi\overline{\xi} = |\xi|^2 > 0$. Furthermore, $\overline{\xi}$ is also a q-th root of unity, and so we see that $\xi\overline{\xi} = 1$ (the only real, positive root of unity is 1). It follows that for any Dirichlet character χ have $\overline{\chi([a])} = \chi([a]^{-1})$. Thus

$$\sum_{\chi \in \mathrm{Dir}(q)} \chi(a)\overline{\chi(b)} = \sum_{\chi \in \mathrm{Dir}(q)} \chi([a][b]^{-1}) = \begin{cases} q - 1 & \text{if } [a][b]^{-1} = 1 \in (\mathbb{Z}/q\mathbb{Z})^\times \\ 0 & \text{otherwise} \end{cases}$$

The condition $ab^{-1} = 1$ is equivalent to $a \equiv b \mod q$, so the claim follows. □

References

[Neu92] Jürgen Neukirch. *Algebraic Number Theory.* Berlin Heidelberg: Springer, 1992.

[Wol] Inc. Wolfram Research. *Wolfram Alpha Online.* Champaign, IL, 2021. URL: `https://www.wolframalpha.com/` (visited on 11/29/2021).