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 1

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*

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

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

Note that property (ii) and (iii) directly follow from the definition, as $\tilde{\chi}(n)$ 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

$$\tilde{\chi}(a)\tilde{\chi}(b) = \chi([a])\chi([b]) = \chi([ab]) = \tilde{\chi}(ab)$$

as also $ab \perp q$.

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

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

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

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

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

So χ is a well-defined group homomorphism and we obviously have $\tilde{\chi} = f$. □

Example 3 (Part 1 (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 $f = \tilde{\chi}$ for the group homomorphism

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

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

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 $\chi' : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$ such that $\chi(\mathbb{N}) = \chi((\mathbb{Z}/q\mathbb{Z})^*) \cup \{0\} \subseteq \mathbb{C}$ 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

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

which is finite. □

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

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

In this case, have that

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

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

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

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

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

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

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

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 $|\tilde{\chi}(n)| \leq C$ for all $n \in \mathbb{N}$. Then

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

which is well-defined and finite for $\Re(s) > 0$. Further, the expression converges uniformly (as a function in s on a neighborhood of 1) to 0 as $X \to \infty$. So

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

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

Applied to our example, we find

Example 6 (Part 1 (ii))**.** *Let $f : \mathbb{N} \to \mathbb{C}$ be the Dirichlet character from Example 3 with corresponding group homomorphism $\chi : (\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{C}$. Then*

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

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 (Part 1 (iii))**.** *There are infinitely many primes p with $p \equiv 3 \mod 4$.*

Proof. It suffices to show that there is a prime number $q \equiv 3 \mod 4$ with $q \geq N$ for every $N \in \mathbb{N}$. Let

$$P := \prod_{p \in \mathbb{P},\ p \leq N} p$$

□

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

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).