

# 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  $\chi : \mathbb{N} \rightarrow \mathbb{C}$  such that

- $\chi$  is completely multiplicative, so  $\chi(a)\chi(b) = \chi(ab)$
- $\chi$  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  $(\mathbb{Z}/q\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$  via

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

*Proof.* First of all, we show that the map is well-defined. Let  $f : (\mathbb{Z}/q\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$  be a (multiplicative) group homomorphism, and we show that  $\chi_f$  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  $n \bmod q$ . 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  $\chi : \mathbb{N} \rightarrow \mathbb{C}$  and construct a group homomorphism  $f : (\mathbb{Z}/q\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ . 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  $\chi_f = \chi$ . □

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

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

is a Dirichlet character.

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

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

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

Now we want to define Dirichlet series of Dirichlet characters.

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

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

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

*Proof.* By Lemma 2, we know that  $\chi$  corresponds to a group homomorphism  $f : (\mathbb{Z}/q\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$  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

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

which is finite. □

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

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

If this is the case, then

$$\lim_{s \rightarrow 1^+} L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n}$$

where the right-hand side converges (but not absolutely).

*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

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

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

For the other direction, assume that  $c = 0$ . We will only consider real  $s$  now. Observe that by Bernoulli's inequality, have for  $0 < s \leq 1$  that

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

If  $s > 1$  and  $k \leq q$ , then also  $(qn)^{-s} - (qn + k)^{-s} = O(sn^{-(1+\epsilon)})$  for some small enough  $0 < \epsilon < 1$ . 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 for all  $s \geq \epsilon$  and  $X \leq Y$  it holds

$$\begin{aligned}
& \sum_{X \leq n \leq Y} \chi(n) n^{-s} \\
&= O(qCX^{-s} + qCY^{-s}) + \sum_{X/q \leq n \leq Y/q} \sum_{0 < k \leq q} \chi(qn + k) \left( (qn)^{-s} + \underbrace{(qn + k)^{-s} - (qn)^{-s}}_{=O(sn^{-(1+\epsilon)})} \right) \\
&= O(qCX^{-s}) + \sum_{X/q \leq n \leq Y/q} \left( (qn)^{-s} + \sum_{0 < k \leq q} O(Csn^{-(1+\epsilon)}) \right) = \\
&= O(qCX^{-s}) + 0 + O\left(Cqs \sum_{X/q \leq n \leq Y/q} n^{-(1+\epsilon)}\right) \\
&= O(qCX^{-s}) + O\left(Cqs \sum_{X/q \leq n} n^{-(1+\epsilon)}\right)
\end{aligned}$$

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

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

as  $X \rightarrow \infty$  (on  $[\epsilon, \infty[$ ). Thus the limit is continuous and extends  $L(s, \chi_f)$  defined on  $]1, \infty[$ . It follows that  $\lim_{t \rightarrow s^+} L(t, \chi_f)$  exists and is equal to  $\sum_{n \geq 1} \chi(n) n^{-s}$ .  $\square$

Applied to our example, we find

**Example 6** (Ex (ii)). Let  $f : \mathbb{N} \rightarrow \mathbb{C}$  be the Dirichlet character from Example 3 with corresponding group homomorphism  $g : (\mathbb{Z}/4\mathbb{Z})^\times \rightarrow \mathbb{C}$ . 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  $\lim_{s \rightarrow 1^+} L(s, f)$  exists. The lemma further yields that

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

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

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

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

Interestingly, we can also study the series

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

using Euler Products.

**Example 7** (Ex (ii)). Have for  $\Re(s) > 1$  that

$$\sum_p \frac{f(p)}{p^s} = \log(L(f, s)) + O(\zeta(2\Re(s)))$$

In particular, we see that

$$\lim_{s \rightarrow 1^+} \sum_p \frac{f(p)}{p^s}$$

exists.

*Proof.* By Taylor series expansion, see that

$$\log(1 - x) = -x + O(|x|^2)$$

Hence for  $\Re(s) > 1$  we can consider the logarithm of the Euler Product to find

$$\begin{aligned} \log(L(f, s)) &= \log\left(\prod_p \sum_{k \geq 0} \frac{f(p^k)}{p^{ks}}\right) = \log\left(\prod_p \frac{1}{1 - f(p)/p^s}\right) \\ &= \sum_p -\log\left(1 - \frac{f(p)}{p^s}\right) = \sum_p \frac{f(p)}{p^s} + O\left(\frac{f(p)^2}{p^{2\Re(s)}}\right) \\ &= \sum_p \frac{f(p)}{p^s} + O\left(\underbrace{\sum_p \frac{f(p)}{p^{2\Re(s)}}}_{\leq \zeta(2\Re(s))}\right) = \sum_p \frac{f(p)}{p^s} + O(\zeta(2\Re(s))) \end{aligned}$$

□

**Lemma 8.** Let  $n \equiv 3 \pmod{4}$ . Then  $n$  has a prime factor  $p \equiv 3 \pmod{4}$ .

*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  $a \not\equiv b \pmod{4}$ . As both  $a$  and  $b$  must be odd, we see that either  $a \equiv 3 \pmod{4}$  or  $b \equiv 3 \pmod{4}$  and the claim follows by the induction hypothesis. □

**Corollary 9** (Ex (iii)). There are infinitely many primes  $p$  with  $p \equiv 3 \pmod{4}$ .

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

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

Thus, by Lemma 8,  $P+2$  has a prime factor  $q \equiv 3 \pmod{4}$ . However,  $q \neq p_i$  as  $p_i \nmid P+2$  for all  $i$  (if  $p_i \mid P+2$ , then  $p_i \mid P+2-P=2$ , a contradiction). This contradicts our assumption.  $\square$

For the case of primes  $\equiv 1 \pmod{4}$ , 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 10.** Let  $q \geq 3$  be an integer. Then there are infinitely many primes  $p$  with  $p \equiv 1 \pmod{q}$ .

*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  $\Phi_q$ . 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  $\omega_q$  (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  $\Phi_q \pmod{p}$  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.  $p \equiv 1 \pmod{q}$ .

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

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

as  $\text{MiPo}_{\mathbb{Q}}(\omega_q) = \prod_{\sigma} (\sigma(\omega_q) - X)$ . Hence,  $\alpha$  is not a unit in  $\mathcal{O}$ . On the other hand,  $(\alpha)$  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  $(\alpha)$  consists only of prime ideals  $(p), p \neq p_i$  and it follows that  $(\alpha) = (n)$  for some integer  $n \geq 2$ . As  $\omega_q$  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.  $\square$

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

**Corollary 11** (Ex (iii)). There are infinitely many primes  $p$  with  $p \equiv 1 \pmod{4}$ .

*Proof.* This is just a special case of Prop. 10. □

**Example 12** (Ex (iii)). Using a computer, we can also study the actual frequency of prime numbers  $\equiv 1, 3 \pmod{4}$  among e.g. the first  $10^8$  integers. This seems to indicate that both numbers are asymptotically equal, which seems natural, given the result of Example 7. For example, there are 332180 primes  $\equiv 1 \pmod{4}$  and 332398 primes  $\equiv 3 \pmod{4}$  smaller than  $10^8$ . To find these numbers, the following python code was used.

```
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  $(\mathbb{Z}/q\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ . If we now assume  $q$  to be prime, we get an even nicer characterization.

So for the whole section, assume that  $q \geq 3$  is a prime.

**Corollary 13** (Ex (i)). Let  $\chi, \chi' : \mathbb{N} \rightarrow \mathbb{C}$  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  $f, f' : (\mathbb{Z}/q\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$  be the associated group homomorphisms of  $\chi, \chi'$  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 14** (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

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

is a well-defined Dirichlet character.

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

Note that the image of a group homomorphism  $f : (\mathbb{Z}/q\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$  is a subgroup of  $\mathbb{C}^\times$ . Using Corollary 13, we can describe it quite concretely.

**Proposition 15.** Let  $\chi : \mathbb{N} \rightarrow \mathbb{C}$  be a Dirichlet character with group homomorphism  $f : (\mathbb{Z}/q\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ . Then  $\text{im } f \leq S$  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  $\text{End}((\mathbb{Z}/q\mathbb{Z})^\times)$  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 13. □

Note that the endomorphism monoid  $\text{End}((\mathbb{Z}/q\mathbb{Z})^\times)$  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 16.** Denote by  $\text{Dir}(q)$  the set of Dirichlet characters modulo  $q$ .

By Corollary 14 each group endomorphism  $f \in \text{End}((\mathbb{Z}/q\mathbb{Z})^\times)$  is determined by its value at a primitive root of unity  $r \in (\mathbb{Z}/q\mathbb{Z})^\times$ , hence

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

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

**Remark 17.** 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 18** (Ex (iii)). Let  $\chi_0$  be the trivial Dirichlet character given by  $r \mapsto 1$ . Then

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

Furthermore, for  $b \not\equiv 1 \pmod{q}$  have

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

*Proof.* Clearly

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

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

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

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

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

where  $\omega \in \mathbb{C}$  is a primitive  $q$ -th root of unity and  $r \in \mathbb{Z}$  is a primitive root modulo  $q$ .

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

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

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

Using these basic results, we can now prove facts on the Dirichlet series of characters.

**Proposition 19** (Ex (iv)). Let  $a \perp q$ . Then for  $\Re(s) > 1$  have

$$\sum_{n \equiv a \pmod{q}} \frac{\Lambda(n)}{n^s} = \frac{1}{q-1} \sum_{\chi \in \text{Dir}(q)} \overline{\chi(a)} \sum_{n \geq 1} \frac{\Lambda(n)\chi(n)}{n^s}$$

(All those series obviously converge absolutely since  $\Re(s) > 1$ )

*Proof.* By Prop. 18 we have for all  $n \in \mathbb{N}$  that

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

It follows that

$$\begin{aligned} \sum_{n \equiv a \pmod{q}} \Lambda(n)n^{-s} &= \sum_{n \geq 1} \Lambda(n)n^{-s} \begin{cases} 1 & \text{if } a \equiv n \pmod{q} \\ 0 & \text{otherwise} \end{cases} \\ &= \sum_{n \geq 1} \Lambda(n)n^{-s} \frac{1}{q-1} \sum_{\chi \in \text{Dir}(q)} \overline{\chi(a)}\chi(n) \\ &= \frac{1}{q-1} \sum_{\chi \in \text{Dir}(q)} \overline{\chi(a)} \sum_{n \geq 1} \Lambda(n)\chi(n)n^{-s} \end{aligned}$$

as infinite summation clearly commutes with finite sums.  $\square$

**Example 20** (Ex (v)). We consider the Dirichlet characters mod 5. A (primitive) 5-th root of unity  $\omega_5 \in \mathbb{C}$  is given by  $\omega_5 = \exp(2\pi i/5)$ . On the other hand, a primitive root modulo 5 is e.g. given by  $r = 2$  since  $2^2 \equiv -1 \pmod{5}$ . Thus we have the trivial Dirichlet character  $\chi_0$  and  $5-1=4$  nontrivial Dirichlet characters mod 5, namely those given by

$$\begin{aligned} \chi_1 : 1 \mapsto 1, 2 \mapsto \omega_5 = \exp(2\pi i/5), 3 \mapsto \omega_5^3 = \exp(6\pi i/5), 4 \mapsto \omega_5^2 = \exp(4\pi i/5), \\ \chi_2 : 1 \mapsto 1, 2 \mapsto \omega_5^2 = \exp(4\pi i/5), 3 \mapsto \omega_5 = \exp(2\pi i/5), 4 \mapsto \omega_5^4 = \exp(8\pi i/5), \\ \chi_3 : 1 \mapsto 1, 2 \mapsto \omega_5^3 = \exp(6\pi i/5), 3 \mapsto \omega_5^4 = \exp(8\pi i/5), 4 \mapsto \omega_5^1 = \exp(2\pi i/5), \\ \chi_4 : 1 \mapsto 1, 2 \mapsto \omega_5^4 = \exp(8\pi i/5), 3 \mapsto \omega_5^2 = \exp(4\pi i/5), 4 \mapsto \omega_5^3 = \exp(6\pi i/5), \end{aligned}$$

### 3 Part III

Again, let  $q \geq 3$  be a prime. Let further  $\chi$  be a Dirichlet character mod  $q$ .

**Proposition 21** (Ex (i)). For  $\Re(s) > 1$  have that

$$\frac{L(s, \chi)'}{L(s, \chi)} = \sum_{n \geq 1} \frac{\Lambda(n) \chi(n)}{n^s}$$

*Proof.* Consider any  $\epsilon > 0$ . The series

$$\sum_{n \geq 1} \frac{d}{ds} \chi(n) n^{-s} = \sum_{n \geq 1} \chi(n) \log(n) n^{-s}$$

converges uniformly on  $\Re(s) \geq 1 + \epsilon$ , as  $|\chi(n)| \leq C$  for some  $C > 0$  and all  $n \in \mathbb{N}$  (by the lecture, we know that  $\sum_n \log(n) n^{-s}$  converges uniformly on  $\Re(s) \geq 1 + \epsilon$ ). Hence, we may interchange summation and differentiation to get

$$L(s, \chi)' = \sum_{n \geq 1} \chi(n) \frac{d}{ds} n^{-s} = \sum_{n \geq 1} \chi(n) \log(n) n^{-s}$$

for  $\Re(s) \geq 1 + \epsilon$ . As  $\epsilon > 0$  was arbitrary, we get

$$L(s, \chi)' = \sum_{n \geq 1} \chi(n) \log(n) n^{-s}$$

for all  $\Re(s) > 1$ .

Furthermore,  $\chi$  and  $\mu$  are multiplicative, and hence so is  $(\chi\mu)(n) := \chi(n)\mu(n)$ . Thus we have the Euler products

$$\sum_{n \geq 1} \mu(n) \chi(n) n^{-s} = \prod_{p \in \mathbb{P}} \sum_{k \in \mathbb{N}} \mu(p^k) \chi(p^k) p^{-sk} = \prod_{p \in \mathbb{P}} (1 - \chi(p) p^{-s})$$

and

$$\sum_{n \geq 1} \chi(n) n^{-s} = \prod_{p \in \mathbb{P}} \sum_{k \in \mathbb{N}} \chi(p^k) p^{-sk} = \prod_{p \in \mathbb{P}} \frac{1}{1 - \chi(p) p^{-s}}$$

Everything converges absolutely for  $\Re(s) > 1$ , and so it follows

$$\frac{1}{L(s, \chi)} = \sum_{n \geq 1} (\chi\mu)(n) n^{-s}$$

By the compatibility of Dirichlet convolution and Dirichlet summation, we now find

$$L(s, \chi)' \frac{1}{L(s, \chi)} = \left( \sum_{n \geq 1} \chi(n) \log(n) n^{-s} \right) \left( \sum_{n \geq 1} \chi(n) \mu(n) n^{-s} \right) = \sum_{n \geq 1} (\chi \log * \chi\mu)(n) n^{-s}$$

and so it is left to show that  $\chi \log * \chi\mu = \chi\Lambda$ .

This is true, as for all  $n \in \mathbb{N}$  it holds

$$\begin{aligned} (\chi \log * \chi \mu)(n) &= \sum_{ab=n} \chi(a) \chi(b) \log(a) \mu(b) \\ &= \sum_{ab=n} \chi(ab) \log(a) \mu(b) = \chi(n) \sum_{ab=n} \log(a) \mu(b) \\ &= \chi(n) (\log * \mu)(n) = (\chi \Lambda)(n) \end{aligned}$$

□

Now we want to find an analytic continuation of  $L(s, \chi)$  to  $\Re(s) > 0$ . First of all, we consider  $\chi_0$ .

**Proposition 22** (Ex (ii)). For  $\Re(s) > 1$  we have

$$L(s, \chi_0) = (1 - q^{-s}) \zeta(s)$$

In particular,  $L(s, \chi_0)$  has a meromorphic continuation to  $\Re(s) > 0$  with only one simple pole at  $s = 1$ .

*Proof.* As  $\chi_0$  is fully multiplicative, we have the Euler product

$$\begin{aligned} L(s, \chi_0) &= \sum_{n \geq 1} \chi_0(n) n^{-s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - \chi_0(p) p^{-s}} = \prod_{p \neq q} \frac{1}{1 - p^{-s}} \\ &= (1 - q^{-s}) \prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}} = (1 - q^{-s}) \zeta(s) \end{aligned}$$

as all products converge absolutely. □

For the other Dirichlet characters, the situation is slightly more complicated. First, we will bound the value of the partial sums of a Dirichlet character.

**Lemma 23** (Ex (iii)). Let  $\chi \neq \chi_0$  be a Dirichlet character mod  $q$  and consider the sum function

$$A(n) := \sum_{1 \leq k \leq n} \chi(k)$$

Then  $|A(n)| \leq q$  for all  $n \in \mathbb{N}$ .

*Proof.* Have

$$\begin{aligned} |A(n)| &= \left| \sum_{1 \leq k \leq n} \chi(k) \right| \leq \left| \sum_{q \lfloor n/q \rfloor < l \leq n} \chi(l) \right| + \underbrace{\left| \sum_{0 \leq k < \lfloor n/q \rfloor} \sum_{0 < l \leq q} \chi(kq + l) \right|}_{=0 \text{ by Prop. 18}} \\ &= \left| \sum_{q \lfloor n/q \rfloor < l \leq n} \chi(l) \right| \leq \sum_{q \lfloor n/q \rfloor < l \leq n} |\chi(l)| = \sum_{q \lfloor n/q \rfloor < l \leq n} 1 \\ &= q(n/q - \lfloor n/q \rfloor) \leq q \end{aligned}$$

for all  $n \in \mathbb{N}$ . □

Now we can show the analytic continuation of  $L(s, \chi)$  to  $\Re(s) > 0$ .

**Proposition 24** (Ex (iv)). Let  $\chi \neq \chi_0$  be a Dirichlet character mod  $q$ . Then

$$L(s, \chi) = s \int_1^\infty A(t) t^{-(s+1)} dt$$

for  $\Re(s) > 1$ . Further, the right-hand side is a holomorphic function on  $\Re(s) > 0$  and thus provides an analytic continuation of  $L(s, \chi)$  to  $\Re(s) > 0$ .

*Proof.* Using partial summation, we find for some  $0 < \epsilon < 1$  that

$$\begin{aligned} \sum_{n \geq 1} \chi(n) n^{-s} &= A(1 - \epsilon)(1 - \epsilon)^{-s} - (-s) \int_{1-\epsilon}^\infty A(t) t^{-(s+1)} dt \\ &= s \int_1^\infty A(t) t^{-(s+1)} dt \end{aligned}$$

Further, the integral converges absolutely by Lemma 23, and thus is holomorphic on  $\Re(s) > 0$ .  $\square$

**Corollary 25** (Ex (iv)). The function  $L(s, \chi)' / L(s, \chi)$  is bounded on a neighborhood of 1, provided that  $L(1, \chi) \neq 0$ .

*Proof.* As  $L(s, \chi)' / L(s, \chi)$  is meromorphic on  $\Re(s) > 0$ , we know that it is holomorphic on some neighborhood of 1 unless it has a pole at  $s = 1$ . In the third exercise class of ANT, it was shown that this would imply  $L(1, \chi) = 0$  or  $L(s, \chi)'$  has a pole at  $s = 1$ .

However, the derivative of a holomorphic function is again holomorphic, so  $L(s, \chi)'$  has no pole at  $s = 1$ . Provided that  $L(1, \chi) \neq 0$ , it follows that  $L(s, \chi)' / L(s, \chi)$  is holomorphic on a compact neighborhood of 1, so bounded.  $\square$

Now we can show the main result of this miniproject. We will prove two auxiliary lemmas before.

**Lemma 26.** For  $a \perp q$ , the function

$$\rho_a(s) := \frac{1}{q-1} \sum_{\chi \in \text{Dir}(q)} \overline{\chi(a)} \sum_{n \geq 1} \frac{\Lambda(n) \chi(n)}{n^s}$$

is a meromorphic function on  $\Re(s) > 0$  with a simple poles at 1 (and possibly other poles on  $\Re(s) > 0$ ).

*Proof.* By Prop. 21, we have for  $\chi \in \text{Dir}(q)$  that

$$\frac{\overline{\chi(a)}}{q-1} \sum_{n \geq 1} \frac{\Lambda(n) \chi(n)}{n^s} = \frac{\overline{\chi(a)}}{q-1} \frac{L(s, \chi)'}{L(s, \chi)}$$

If  $\chi \neq \chi_0$ , then Corollary 25 shows that this function has no pole at  $s = 1$ .

If  $\chi = \chi_0$  on the other hand, Prop. 22 shows that

$$L(s, \chi_0) = (1 - q^{-s})\zeta(s)$$

Hence

$$\frac{L(s, \chi_0)'}{L(s, \chi_0)} = \frac{\log(q)q^{-s}\zeta(s) + (1 - q^{-s})\zeta'(s)}{(1 - q^{-s})\zeta(s)} = \frac{\log(q)}{q^s - 1} + \frac{\zeta'(s)}{\zeta(s)}$$

has a simple pole at  $s = 1$ . Since  $a \perp q$ , we see that  $\chi_0(a) = 1$  and thus also

$$\frac{\overline{\chi_0(a)}}{q-1} \sum_{n \geq 1} \frac{\Lambda(n)\chi_0(n)}{n^s} = \frac{\overline{\chi_0(a)}}{q-1} \frac{L(s, \chi_0)'}{L(s, \chi_0)}$$

has a simple pole at  $s = 1$ .

Together, this yields that the sum of those functions

$$\rho_a(s) = \frac{1}{q-1} \sum_{\chi \in \text{Dir}(q)} \overline{\chi(a)} \sum_{n \geq 1} \frac{\Lambda(n)\chi(n)}{n^s}$$

is a meromorphic function with a simple pole at  $s = 1$ . □

**Lemma 27.** Let  $a \perp q$  and define

$$\Psi_a(x) := \sum_{n < x, n \equiv a \pmod q} \Lambda(n)$$

and

$$\theta_a(x) := \sum_{p < x, p \equiv a \pmod q} \log(p)$$

Then

$$\Psi_a(x) - \theta_a(x) = O(x^{1/2} \log(x))$$

*Proof.* Have

$$\begin{aligned} \Psi_a(x) - \theta_a(x) &= \sum_{p^k < x, p^k \equiv a \pmod q} \log(p) - \sum_{p < x, p \equiv a \pmod q} \log(p) \\ &= \sum_{p^k < x, k \geq 2, p^k \equiv a \pmod q} \log(p) \leq \sum_{p^k < x, k \geq 2} \log(p) \\ &= \Psi(x) - \theta(x) = O(x^{1/2} \log(x)) \end{aligned}$$

where the last equality was proven in the lecture. □

**Proposition 28** (Ex (v)). Assume that  $L(1, \chi) \neq 0$  for all  $\chi \in \text{Dir}(q) \setminus \{\chi_0\}$ . Then for all  $a \perp q$  there are infinitely many primes  $p \equiv a \pmod q$ .

*Proof.* Assume not, then  $\theta_a(x)$  is bounded, i.e.  $\theta_a(x) = O(1)$ . With Lemma 27 it follows that  $\Psi_a(x) = O(x^{1/2} \log x)$ .

By Prop. 19 we have that for  $\Re(s) > 1$

$$\rho_a(s) = \sum_{n \equiv a \pmod{q}} \Lambda(n) n^{-s}$$

Partial summation yields that for  $\Re(s) > 1$  have

$$\begin{aligned} \rho_a(s) &= \sum_{n \equiv a \pmod{q}} \Lambda(n) n^{-s} \\ &= \lim_{t \rightarrow \infty} \left( \underbrace{t^{-s} \sum_{n < t, n \equiv a \pmod{q}} \Lambda(n)}_{=t^{-s} \Psi_a(t) = t^{-s} O(t \log t) = o(1)} \right) + s \int_1^\infty \left( \underbrace{\sum_{n < t, n \equiv a \pmod{q}} \Lambda(n)}_{=\Psi_a(t)} \right) t^{-(s+1)} dt \\ &= s \int_1^\infty \Psi_a(t) t^{-s-1} dt = s \int_1^\infty O(t^{1/2} \log t) t^{-s-1} dt \\ &= O \left( |s| \int_1^\infty \log(t) t^{-\Re(s)-1/2} dt \right) \\ &= O \left( |s| \left( \frac{1}{1/2 - \Re(s)} 1^{1/2 - \Re(s)} + \frac{1}{1/2 - \Re(s)} \int_1^\infty t^{-\Re(s)-1/2} dt \right) \right) \\ &= O \left( |s| \frac{1}{(1/2 - \Re(s))^2} \right) \end{aligned}$$

However this function has no pole at  $s = 1$ , a contradiction to Lemma 26.  $\square$

**Example 29** (Ex (vi)). For all the nontrivial Dirichlet characters  $\chi_1, \dots, \chi_4$  defined in Example 20, we have

$$L(1, \chi_i) \neq 0$$

It follows that there are infinitely many primes  $\equiv a \pmod{5}$ , for all  $a \perp 5$ .

*Proof.* By Prop. 5 we know that

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

For the fifth root of unity  $\omega \in \mathbb{C}$  such that  $\chi_i(1) = \omega$ , we thus find

$$\begin{aligned} L(1, \chi_i) &= \sum_{k \geq 0} \sum_{1 \leq n \leq 4} \frac{\chi(5k+n)}{(5k+n)^s} = \sum_{k \geq 0} \frac{\omega}{(5k+1)^s} + \frac{\omega^2}{(5k+2)^s} + \frac{\omega^3}{(5k+3)^s} + \frac{\omega^4}{(5k+4)^s} \\ &= \sum_{k \geq 0} \omega \left( \underbrace{\frac{1}{(5k+1)^s} - \frac{1}{(5k+4)^s}}_{>0} \right) + \omega^2 \left( \underbrace{\frac{1}{(5k+2)^s} - \frac{1}{(5k+3)^s}}_{>0} \right) \end{aligned}$$

Hence we have positive coefficients  $a_k, b_k > 0$  with

$$L(1, \chi_i) - \sum_{k \geq 0} a_k \omega + b_k \omega^2 = \omega \sum_{k \geq 0} a_k + b_k \omega$$

In particular,

$$\Im \left( \frac{L(1, \chi_i)}{\omega} \right) = \sum_{k \geq 0} b_k \Im(\omega) = \Im(\omega) \underbrace{\sum_{k \geq 0} b_k}_{>0}$$

Since  $\chi_i$  is a nontrivial Dirichlet character, we see that  $\Im(\omega) \neq 0$  and so  $\Im(L(1, \chi_i)/\omega) \neq 0$ , thus  $L(1, \chi_i) \neq 0$ .  $\square$

**Remark 30** (Ex (vii)). TODO

## 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).