Notes on the Finite Fourier Transform

Peter Woit
Department of Mathematics, Columbia University
woit@math.columbia.edu

April 28, 2020

1 Introduction

In this final section of the course we'll discuss a topic which is in some sense much simpler than the cases of Fourier series for functions on S^1 and the Fourier transform for functions on $\mathbf{R}$, since it will involve functions on a finite set, and thus just algebra and no need for the complexities of analysis. This topic has important applications in the approximate computation of Fourier series (which we won't cover), and in number theory (which we'll say a little bit about).

2 The group $\mathbf{Z}(N)$

What we'll be doing is simplifying the topic of Fourier series by replacing the multiplicative group

$$S^1 = \{z \in \mathbf{C} : |z| = 1\}$$

by the finite subgroup

$$\mathbf{Z}(N) = \{z \in \mathbf{C} : z^N = 1\}$$

If we write $z = re^{i\theta}$, then

$$\begin{aligned} z^N = 1 &\implies r^N e^{i\theta N} = 1 \\ &\implies r = 1, \quad \theta N = k2\pi \ (k \in \mathbf{Z}) \\ &\implies \theta = \left(\frac{k}{N}2\pi\right)_{\text{mod } 2\pi} \qquad k = 0, 1, 2, \cdots, N-1 \end{aligned}$$

The group $\mathbf{Z}(N)$ is thus explicitly given by the set

$$\mathbf{Z}(N) = \{1, e^{i\frac{2\pi}{N}}, e^{i2\frac{2\pi}{N}}, \cdots, e^{i(N-1)\frac{2\pi}{N}}\}$$

Geometrically, these are the points on the unit circle one gets by starting at 1 and dividing it into N sectors with equal angles $\frac{2\pi}{N}$.

(Draw a picture, $N = 6$)

The set $\mathbf{Z}(N)$ is a group, with

- identity element 1 ($k = 0$)
- inverse
$$(e^{2\pi i \frac{k}{N}})^{-1} = e^{-2\pi i \frac{k}{N}} = e^{2\pi i \frac{(N-k)}{N}}$$
- multiplication law
$$e^{ik\frac{2\pi}{N}} e^{il\frac{2\pi}{N}} = e^{i(k+l)\frac{2\pi}{N}}$$

One can equally well write this group as the additive group $(\mathbf{Z}/N\mathbf{Z}, +)$ of integers mod N, with isomorphism

$$\begin{aligned} \mathbf{Z}(N) &\leftrightarrow \mathbf{Z}/N\mathbf{Z} \\ e^{ik\frac{2\pi}{N}} &\leftrightarrow [k]_N \\ 1 &\leftrightarrow [0]_N \\ e^{-ik\frac{2\pi}{N}} &\leftrightarrow -[k]_N = [-k]_N = [N-k]_N \end{aligned}$$

3 Fourier analysis on $\mathbf{Z}(N)$

An abstract point of view on the theory of Fourier series is that it is based on exploiting the existence of a particular othonormal basis of functions on the group S^1 that are eigenfunctions of the linear transformations given by rotations. The orthonormal basis elements are the $e_m = e^{in\theta},\ m \in \mathbf{Z}$, recalling that

$$\langle e_n, e_m \rangle = \frac{1}{2\pi} \int_{-\pi}^{\pi} e^{in\theta} e^{-im\theta} d\theta = \delta_{n,m}$$

Rotation by an angle ϕ acts on the circle S^1 by

$$\theta \to \theta + \phi$$

and on functions on the circle by the linear transformation

$$f(\theta) \to (T_\phi f)(\theta) = f(\theta + \phi)$$

(note that the rotation transformation on S^1 itself is not a linear transformation, since S^1 is not a linear space). The functions e_n are eigenfunctions of T_ϕ, since

$$(T_\phi e_n)(\theta) = e^{in(\theta+\phi)} = e^{in\phi} e^{in\theta} = e^{in\phi} e_n$$

We would like to do the same thing for functions on $\mathbf{Z}(N)$: find an orthornormal set of such functions that are eigenvalues for the action of the set $\mathbf{Z}(N)$ on itself by discrete rotations. We'll write a complex-valued function on $\mathbf{Z}(N)$ as

$$F : [k] \in \mathbf{Z}(N) \to F(k) \in \mathbf{C},\ F(k) = F(k+N)$$

For inner product we'll take

$$\langle F, G \rangle = \sum_{k=0}^{N-1} F(k) \overline{G(k)}$$

so

$$||F||^2 = \sum_{k=0}^{N-1} |F(k)|^2$$

With these choices we have

Claim. *The functions* $e_l : \mathbf{Z}(N) \to \mathbf{C}$ *given by*

$$e_l(k) = e^{i2\pi \frac{lk}{N}}$$

for $l = 0.1, 2, \cdots, N-1$ *satisfy*

$$\langle e_l, e_m \rangle = N\delta_{l,m}$$

so the functions

$$e_l^* = \frac{1}{\sqrt{N}} e_l$$

are orthonormal. They form a basis since there are N *of them and the space of functions on* $\mathbf{Z}(N)$ *is* N*-dimensional.*

Proof. First define

$$W_N = e^{i\frac{2\pi}{N}}$$

then

$$\begin{aligned} \langle e_l, e_m \rangle &= \sum_{k=0}^{N-1} e^{i\frac{2\pi}{N}lk} e^{-i\frac{2\pi}{N}mk} \\ &= \sum_{k=0}^{N-1} (W_N)^{(l-m)k} \end{aligned}$$

If $l = m$ this is a sum of N 1's, so

$$\langle e_l, e_m \rangle = N$$

If $l \neq m$, let $q = W_N^{l-m}$. Then the sum is

$$\langle e_l, e_m \rangle = 1 + q + q^2 + \cdots + q^{N-1} = \frac{1 - q^N}{1 - q}$$

but this is 0 since $q^N = (W_N)^N = 1$. □

Our analog of the Fourier series

$$F(\theta) = \sum_{n=-\infty}^{\infty} a_n e^{in\theta}$$

for a function F on S^1 will be writing a function on $\mathbf{Z}(N)$ in terms of the orthonormal basis $\{e_n^*\}$, as

$$\begin{aligned} F(k) &= \sum_{n=0}^{N-1} \langle F, e_n^* \rangle e_n^* \\ &= \sum_{n=0}^{N-1} \langle F, e_n^* \rangle \frac{1}{\sqrt{N}} e^{i2\pi \frac{nk}{N}} \end{aligned}$$

The analog of the Fourier coefficients

$$a_n = \widehat{f}(n) = \frac{1}{2\pi} \int_{-\pi}^{\pi} F(\theta) e^{-in\theta}$$

will be the finite set of numbers

$$\begin{aligned} \widehat{F}(n) &= \frac{1}{\sqrt{N}} \langle F, e_n^* \rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} F(k) \frac{1}{\sqrt{N}} e^{-i2\pi \frac{kn}{N}} \\ &= \frac{1}{N} \sum_{k=0}^{N-1} F(k) e^{-i2\pi \frac{kn}{N}} \end{aligned}$$

for $n = 0, 1, 2, \cdots, N-1$. Here the Fourier inversion theorem is automatic, just the usual fact that for finite dimensional vector spaces the coefficients of a vector with respect to an othonormal basis are given by the inner products of the vector with the basis elements.

For another perspective on this, note that there are two distinguished orthonormal bases for functions on $\mathbf{Z}(N)$

- the N functions of k given by

  $$\delta_{kl} = \begin{cases} 1 & k = l \\ 0 & k \neq l \end{cases}$$

  for $l = 0, 1, 2, \cdots, N-1$.

- the N functions of k given by

  $$\frac{1}{\sqrt{N}} e^{i2\pi \frac{kl}{N}}$$

  for $l = 0, 1, 2, \cdots, N-1$.

The Fourier transform for $\mathbf{Z}(N)$ that takes

$$\mathcal{F} : \{F(0), F(1), \cdots, F(N-1)\} \to \{\widehat{F}(0), \widehat{F}(1), \cdots \widehat{F}(N-1)\}$$

is just the change of basis matrix between the above two bases. It can be written as an $N \times N$ complex matrix.

The Plancherel (or Parseval) theorem in this case is automatic from linear algebra: in the complex case, a change of basis between two orthonormal bases is given by a unitary matrix. Note that the way we have defined things, the coefficients with respect to the second orthonormal basis are given by the function $\sqrt{N}\widehat{F}$, not $\widehat{F}$, so the theorem says that

$$\sum_{k=0}^{N-1} |F(k)|^2 = \sum_{k=0}^{N-1} |\sqrt{N}\widehat{F}(k)|^2 = N \sum_{k=0}^{N-1} |\widehat{F}(k)|^2$$

Just as for Fourier series and transforms, one can define a convolution product, in this case by

$$(F * G)(k) = \sum_{l=0}^{N-1} F(k-l)G(l)$$

and show that the Fourier transform takes the convolution product to the usual point-wise product.

4 Fourier analysis on commutative groups

The cases that we have seen of groups $G = S^1, \mathbf{R}, \mathbf{Z}(N)$, are just special cases of a general theory that works for any commutative group, i.e. any set with an associative, commutative ($ab = ba$) multiplication, with an identity element and inverses. When the set is finite, this general theory is very straightforward, but for infinite sets like S^1 and $\mathbf{R}$ one needs to take into account more complicated issues (e.g. those of analysis that we have run into).

The general theory starts with the definition

Definition (Group character)**.** *A character of a group G is a function*

$$e : G \to \mathbf{C}^*$$

such that

$$e(ab) = e(a)e(b)$$

(one says that e is a "homomorphism"). Here $\mathbf{C}^*$ is the multiplicative group of non-zero elements of $\mathbf{C}$.

When G is a finite goup, all elements will have finite order ($a^n = 1$ for some n) and thus

$$e(a^n) = e(a)^n = 1$$

so characters will take as values not general non-zero complex numbers, but n'th roots of unity, so in the subgroup $U(1) \subset \mathbf{C}^*$ of elements of the form $e^{i\theta}$. Such characters will be called "unitary characters".

For the case of $G = \mathbf{Z}(N)$, the

$$e_l(k) = e^{i2\pi \frac{lk}{N}}$$

are characters, since

$$e_l(k)e_l(m) = e_l(k+m)$$

We will denote the set of unitary characters of a group G by $\widehat{G}$, and we have

Claim. *$\widehat{G}$ is a commutative group. It will be called the "character group" of G.*

Proof. $1 \in \widehat{G}$ is the identity function $e(a) = 1$, multiplication is given by

$$(e_1 \cdot e_2)(a) = e_1(a)e_2(a)$$

and the inverse of a character e is given by

$$e^{-1}(a) = (e(a))^{-1}$$

□

Some of the examples we have seen so far of pairs G and $\widehat{G}$ are

- The group $G = \mathbf{Z}(N)$, with elements $k = 0, 1, \cdots, N-1$, has character group $\widehat{G} = \mathbf{Z}(N)$, which has elements e_l for $l = 0, 1, \cdots, N-1$ given by the functions
$$e_l(k) = e^{i2\pi \frac{kl}{N}}$$
- The group $G = S^1$, with elements $e^{i\theta}$, has character group $\widehat{G} = \mathbf{Z}$, with the integer n corresponding to the function
$$e_n(\theta) = e^{in\theta}$$
- The group $G = \mathbf{R}$. with elements x, has character group $\widehat{G} = \mathbf{R}$, which has elements e_p for $p \in \mathbf{R}$ given by the functions
$$e_p(x) = e^{i2\pi px}$$

For finite groups one can define an inner product on $\widehat{G}$ by

$$\langle e, e' \rangle = \frac{1}{|G|} \sum_{a \in G} e(a)\overline{e'(a)}$$

where e, e' are characters of G. These have the property

Claim. *Distinct elements of $\widehat{G}$ are orthonormal.*

Proof. For $e = e'$, one has

$$\langle e, e \rangle = \frac{1}{|G|} \sum_{a \in G} e(a)\overline{e(a)} = \frac{1}{|G|} \sum_{a \in G} 1 = 1$$

For $e \neq e'$ one has

$$\begin{aligned}\langle e, e' \rangle &= \frac{1}{|G|} \sum_{a \in G} e(a)\overline{e'(a)} \\ &= \frac{1}{|G|} \sum_{a \in G} e(a)(e'(a))^{-1}\end{aligned}$$

Picking an element $b \in G$ such that $e(b) \neq e'(b)$ (possible since e, e' are different functions) and using the fact that multiplication of all elements by b is just a relabeling of the group elements, the above gives

$$\begin{aligned}&= \frac{1}{|G|} \sum_{a \in G} e(ba)(e'(ba))^{-1} \\ &= \frac{1}{|G|} \sum_{a \in G} e(b)e(a)(e'(a))^{-1}(e'(b))^{-1} \\ &= e(b)(e'(b))^{-1} \frac{1}{|G|} \sum_{a \in G} e(a)(e'(a))^{-1}\end{aligned}$$

So we have shown

$$\langle e, e' \rangle = e(b)(e'(b))^{-1} \langle e, e' \rangle$$

but by assumption we have

$$e(b)(e'(b))^{-1} \neq 1$$

so we must have $\langle e, e' \rangle = 0$. □

Somewhat harder to prove is that the unitary characters are complete, giving a basis for functions on G. For a proof of this, see pages 233-234 of [1].

We can now define the Fourier transform for any finite commutative group G

Definition. *The Fourier transform for a finite commutative group G takes the function f on G to the function*

$$\mathcal{F}f = \widehat{f}(e) = \langle f, e \rangle = \frac{1}{|G|} \sum_{a \in G} f(a)\overline{e(a)}$$

The Fourier inversion formula again is just the expansion of the function in the orthnormal basis of characters

$$f = \sum_{e \in \widehat{G}} \widehat{f}(e)e = \mathcal{F}^{-1}f$$

$\mathcal{F}$ is just the transformation of basis matrix between the basis of characters and the basis of "δ-functions" (= 1 on one element, 0 on the others). It will be given by a unitary $|G| \times |G|$ matrix, implying a Plancherel/Parseval theorem

$$||f||^2 = \frac{1}{|G|} \sum_{a \in G} |f(a)|^2 = \sum_{e \in \widehat{G}} |\widehat{f}(e)|^2 = ||\widehat{f}||^2$$

One can define a convolution product by

$$f * g(a) = \frac{1}{|G|} \sum_{b \in G} f(ab^{-1}) g(b)$$

which will satisfy

$$\widehat{f * g} = \widehat{f}\widehat{g}$$

Note that

$$e * e' = \begin{cases} e \ if \ e = e' \\ 0 \ if \ e \neq e' \end{cases}$$

So

$$f \to f * e$$

is a projection map, onto the subspaece of functions ϕ on G that are eigenvectors for the linear transformation

$$\phi(a) \to (T_b \phi)(a) = \phi(ba)$$

with eigenalue $e(b)$.

Given two groups G_1 and G_2, one can form a new group, the product group $G_1 \times G_2$. This is the group with elements pairs

$$(a_1, a_2), \quad a_1 \in G_1, \ a_2 \in G_2$$

and multiplication law

$$(a_1, a_2)(b_1, b_2) = (a_1 a_2, b_1 b_2)$$

It is not hard to show that for finite commutative groups the character groups satisfy

$$\widehat{G_1 \times G_2} = \widehat{G_1} \times \widehat{G_2}$$

We won't cover this in this course since it would take us too far afield into algebra, but in a standard abstract algebra course you will learn a theorem that says that any finite commutative group G is isomorphic to the product group

$$\mathbf{Z}(N_1) \times \mathbf{Z}(N_2) \times \cdots \times \mathbf{Z}(N_k)$$

for some positive integers $N_1, N_2, \ldots, N_k$. Its character group $\widehat{G}$ will then by the above be

$$\widehat{\mathbf{Z}(N_1)} \times \widehat{\mathbf{Z}(N_2)} \times \cdots \times \widehat{\mathbf{Z}(N_k)}$$

We see that for a general finite commutative group G and $\widehat{G}$ will be isomorphic and the example we have worked out of $\mathbf{Z}(N)$ is fundamental: the general case is just a product of these for different N. In the next section though, we will see that given an interesting finite commutative group, finding its decomposition into $\mathbf{Z}(N)$ factors can be quite non-trivial.

One generalization of these ideas is to the case of general commutative groups, not necessarily finite. Here one can get into quite complicated questions in analysis, some of which we have seen in the cases $G = S^1$ and $G = \mathbf{R}$. An even larger generalization is to the case of non-commutative groups. To get an analog there for Fourier analysis, one needs to consider not just characters

$$e : G \to U(1)$$

but more general maps

$$\pi : G \to U(n)$$

satisfying the homomorphism property

$$\pi(a)\pi(b) = \pi(ab)$$

where $U(n)$ is the group of unitary $n \times n$ matrices. Identifying all such π is a difficult problem, but once one does so, for each such π one gets an $n \times n$ matrix-valued function on G. The analog of Fourier analysis in this case is the decomposition of arbitrary functions on G in terms of the functions given by the matrix elements of these matrix-valued functions.

5 Fourier analysis on $\mathbf{Z}^*(q)$

We'll now turn to some applications of the finite Fourier transform in analysis. These are based on considering not the additive structure on $\mathbf{Z}(N)$, but the multiplicative structure. One can define a multiplication on the set $\mathbf{Z}(N)$ by

$$[l]_N \cdot [m]_N = [lm]_N$$

This product is commutative, associative, and there's an identity element ($[1]_N$). This makes $\mathbf{Z}(N)$ an example of what algebraists call a "ring." The problem though is that many elements of $\mathbf{Z}(N)$ have no multiplicative inverse. For example, if one takes $N = 4$ and looks for an integer m such that

$$([2]_4)^{-1} = [m]_4$$

the integer m must satisfy

$$[2]_4 \cdot [m]_4 = [2m]_4 = [1]_4$$

But this can't possibly work since $2m$ is even and 1 is odd.

We can however go ahead and define a group by just taking the elements of $\mathbf{Z}(N)$ that do have a multiplicative inverse (such elements are called "units" of the ring $\mathbf{Z}(N)$).

Definition. *The group $\mathbf{Z}^*(q)$ is the set of $[l]_q$ of elements of $\mathbf{Z}(q)$ that have a multiplicative inverse, with the group law multiplication mod q.*

For an alternate characterization of $\mathbf{Z}^*(q)$, first recall that every positive integer $N > 1$ can be uniquely factored in primes, meaning

$$N = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

For any integers a and b we can define

$$\gcd(a, b)$$

to be the largest integer that divides both a and b. If $\gcd(a, b) = 1$ we say that "a and b are relatively prime". This is equivalent to saying that they have no prime factors in common. The group $\mathbf{Z}^*(q)$ could instead have been defined as

$$\mathbf{Z}^*(q) = \{[l]_q \in \mathbf{Z}(q) : \gcd(l, q) = 1\}$$

To see one direction of the equivalence with the other definition, that an element $[l]_q \in \mathbf{Z}(q)$ having an inverse implies that l and q are relatively prime, start by assuming they aren't relatively prime, which means

$$l = pn_1, \quad q = pn_2$$

for some prime p and integers n_1, n_2. In order to find an inverse of $[l]_q$, we need to find an integer m such that

$$[lm]_q = [1]_q$$

which means that

$$lm = nq + 1$$

for some integer n. Under the assumption $\gcd(l, q) \neq 1$ we find that we need to solve

$$pn_1 m = npn_2 + 1$$

which implies

$$n_1 m = nn_2 + \frac{1}{p}$$

but the left hand side is an integer, while the right hand side is a non-trivial fraction. The contradiction implies there is no inverse.

The number of elements of $\mathbf{Z}^*(q)$ is the number of elements of $\{1, 2, \cdots, q-1\}$ that are relatively prime to q. This number defines the Euler ϕ or "totient" function, i.e.

$$\phi(q) = |\mathbf{Z}^*(q)|$$

If q is a prime p, then $1, 2, \ldots, p-1$ are relatively prime to p and all $p-1$ elements of the set

$$[1]_p, [2]_p, \cdots [p-1]_p$$

have multiplicative inverses. In this case one can show (although we won't do it here) that the multiplicative group $\mathbf{Z}^*(p)$ is isomorphic to the additive group

$\mathbf{Z}(p-1)$. As noted before, there is a general theorem that any finite commutative group is isomorphic to a product of groups $\mathbf{Z}(N_j)$ for various N_j.

For any given q that isn't prime, finding the integers N_j and the isomorphism is a non-trivial problem. One can easily though work out what happens for small q. For example, if $q = 4$ we find that $\mathbf{Z}^*(4)$ has two elements

$$[1]_4, [3]_4$$

(since $1, 3$ are the only integers from 0 to 3 relatively prime to 4). One can see that there is an isomorphism of groups between $\mathbf{Z}^*(4)$ and $\mathbf{Z}(2)$ given by

$$[1]_4 \leftrightarrow ([0]_2, +)$$

$$[3]_4 \leftrightarrow ([1]_2, +)$$

since the first of these is the identity, the second an element that squares to the identity

$$[3]_4 \cdot [3]_4 = [9]_4 = [1]_4 \leftrightarrow [1]_2 + [1]_2 = [2]_2 = [0]_2$$

By the general theory, the character group $\widehat{\mathbf{Z}^*(q)}$ has $\phi(q)$ elements. These can be thought of as functions $e(k)$ on the classes $[k]_q$, which are only non-zero. on the k that are relatively prime to q. In number theory these characters appear as "Dirichlet characters", defined for all integers m by

$$\chi_e(m) = \begin{cases} e([m]_q), & \gcd(m, q) = 1 \\ 0, & \gcd(m, q) \neq 1 \end{cases}$$

By the homomorphism property of characters, these are multiplicative functions on $\mathbf{Z}$, satisfying

$$\chi_e(nm) = \chi_e(n)\chi_e(m)$$

6 The zeta function, primes and Dirichlet's theorem

Recall that earlier on in this course we studied the zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

using Poisson summation to derive the functional equation for $\zeta(s)$. One of the main applications of the zeta function is to the study of the distribution of prime numbers, based on

Claim (Euler product formula)**.** *For $s > 1$*

$$\prod_{primes\ p} \frac{1}{1 - p^{-s}} = \zeta(s)$$

Proof. The geometric series formula gives

$$\frac{1}{1-\frac{1}{p^s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots$$

Taking the infinite product

$$\prod_{\text{primes } p_j} (1 + \frac{1}{p_j^s} + \frac{1}{p_j^{2s}} + \frac{1}{p_j^{3s}} + \cdots)$$

for $p_1 < p_2 < \cdots$, and writing this out as a sum of terms, one gets all terms of the form

$$\frac{1}{p_1^{n_1}} \frac{1}{p_2^{n_2}} \cdots \frac{1}{p_k^{n_k}}$$

with coefficient 1, each raised to the power s. By unique factorization of integers this sum is the same sum as

$$\sum_{n=1}^{\infty} \frac{1}{n^s}$$

□

This can be used to give a proof that there are an infinite number of primes (of course there is a much simpler proof by contradiction: multiply all primes and add 1). The argument is that we know that

$$\lim_{s \to 1^+} \zeta(s) = 1 + \frac{1}{2} + \frac{1}{3} + \cdots = \infty$$

but by the Euler product formula, this is

$$\lim_{s \to 1^+} \prod_{\text{primes } p} \frac{1}{1-p^{-s}}$$

which can only be infiinite if the number of primes is infinite. For a more difficult example, there's

Claim. *The sum*

$$\sum_{primes\ p} \frac{1}{p}$$

diverges.

Proof. Taking the logarithm of the Euler product formula

$$\prod_{\text{primes } p} \frac{1}{1-p^{-s}} = \zeta(s)$$

one finds

$$\ln(\zeta(s)) = -\sum_p \ln(1-p^{-s})$$

Using the power series expansion

$$\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots$$

one has the inequality (for $|x| < \frac{1}{2}$)

$$\begin{aligned} |\ln(1+x) - x| &< \frac{x^2}{2}(1 + |x| + |x|^2 + \cdots) \\ &< \frac{x^2}{2}(1 + \frac{1}{2} + (\frac{1}{2})^2 \cdots) \\ &= \frac{x^2}{2}(\frac{1}{1-\frac{1}{2}}) = x^2 \end{aligned}$$

So

$$|\ln(1-p^{-s}) - p^{-s}| < p^{-2s}$$

which implies that in the sum above one can replace $\ln(1-p^{-s})$ by $\frac{1}{p^s}$, changing the result by at most

$$\sum_p \frac{1}{p^{2s}}$$

But

$$\sum_p \frac{1}{p^{2s}} < \sum_{n=1}^{\infty} \frac{1}{n^{2s}} = \zeta(2s)$$

and

$$\lim_{s \to 1^+} \zeta(2s) = \zeta(2) = \frac{\pi^2}{6}$$

which is finite. So

$$\lim_{s \to 1^+} \sum_p \frac{1}{p^s}$$

is infinite, since it differs by less than a finite constant from

$$\lim_{s \to 1^+} \ln(\zeta(s))$$

which we know to be infinite.

□

For more subtle aspects of the distribution of primes, one can define a generalization of the zeta function, which uses the characters of $\mathbf{Z}^*(q)$. These are called Dirichlet L-functions, and defined by

Definition (Dirichlet L-function)**.** *For χ a Dirichlet character, the corresponding Dirichlet L-function is*

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

By much the same argument as for the Euler product formula, these satisfy a product formula

$$L(\chi, s) = \prod_{\text{primes } p} \frac{1}{1 - \chi(p)p^{-s}}$$

By studying the logarithm of this and its limit as $s \to 1^+$, and exploiting Fourier analys on $\mathbf{Z}^*(q)$, one can show

Theorem (Dirichlet's theorem)**.** *For a fixed l and q*

$$\lim_{s \to 1^+} \sum_{primes\ p:[p]_q = l} \frac{1}{p^s}$$

diverges, which implies that there is an infinite number of primes in any arithmetic progression (sequence of the form $\{l, l + q, l + 2q, \cdots\}$).

Proof. The proof is rather complicated and we won't have time to go through it this semester. It can be found in chapter 8 of [1]. □

References

[1] Stein, Elias M. and Shakarchi, Rami, Fourier Analysis: An Introduction. Princeton University Press, 2003.