Math 229: Introduction to Analytic Number Theory

Primes in arithmetic progressions: Dirichlet characters and L-functions

Dirichlet extended Euler's analysis from $\pi(x)$ to

$$\pi(x, a \bmod q) := \#\{p \le x : p \text{ is a positive prime congruent to } a \bmod q\}.$$

We introduce his approach with the example of the distribution of primes mod 4, that is, of $\pi(x, 1 \bmod 4)$ and $\pi(x, 3 \bmod 4)$. The sum of these is of course $\pi(x)-1$ once $x \ge 2$, and we have already obtained

$$s \int_1^\infty \pi(y) y^{-1-s}\, dy = \log \frac{1}{s-1} + O_{s_0}(1) \qquad (1 < s \le s_0) \tag{1}$$

from the Euler product for $\zeta(s)$. By omitting the factor $(1-2^{-s})^{-1}$ we obtain a product formula for

$$(1-2^{-s})\zeta(s) = 1 + 3^{-s} + 5^{-s} + 7^{-s} + \cdots .$$

If we try to estimate $\pi(\cdot, 1 \bmod 4)$ (or $\pi(\cdot, 3 \bmod 4)$) in the same way, we are led to the sum of n^{-s} over the integers all of whose prime factors are are congruent to 1 (or 3) mod 4, which is hard to work with. But we can analyze the *difference* $\pi(x, 1 \bmod 4) - \pi(x, 3 \bmod 4)$ using an Euler product for the *L-series*

$$L(s, \chi_4) := 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + - \cdots = \sum_{n=1}^\infty \chi_4(n) n^{-s}.$$

Here χ_4 is the function

$$\chi_4(n) = \begin{cases} +1, & \text{if } n \equiv +1 \bmod 4; \\ -1, & \text{if } n \equiv -1 \bmod 4; \\ 0, & \text{if } 2|n. \end{cases}$$

This function is (strongly[1]) *multiplicative*:

$$\chi_4(mn) = \chi_4(m)\chi_4(n) \qquad (\text{all } m, n \in \mathbf{Z}). \tag{2}$$

Therefore $L(s, \chi_4)$ factors as did $\zeta(s)$:

$$L(s, \chi_4) = \prod_{p \text{ prime}} \Big(\sum_{c_p=1}^\infty \chi(p^{c_p}) p^{-c_p s} \Big) = \prod_{p \text{ prime}} \frac{1}{1 - \chi(p) p^{-s}}. \tag{3}$$

By comparison with the Euler product for $\zeta(s)$ we see that the manipulations in (3) are valid for $s > 1$ (and in fact for s of real part > 1). Unlike $\zeta(s)$, the function $L(s, \chi_4)$ remains bounded as $s \to 1+$, because the sum $\sum_{n=1}^\infty \chi_4(n) n^{-s}$ may be grouped as

[1] Often a function f is called multiplicative when $f(mn) = f(m)f(n)$ only for coprime m, n; see the Exercises.

$$\Big(1-\frac{1}{3^s}\Big)+\Big(\frac{1}{5^s}-\frac{1}{7^s}\Big)+\Big(\frac{1}{9^s}-\frac{1}{11^s}\Big)+\cdots$$

in which the n-th term is $O(n^{-(s+1)})$ (why?). Indeed this regrouping lets us extend $L(\cdot,\chi_4)$ to a continuous function on $(0,\infty)$. Moreover, each of the terms $(1-3^{-s})$, $(5^{-s}-7^{-s})$, $(9^{-s}-11^{-s})$,... is positive, so $L(s,\chi_4)>0$ for all $s>0$, in particular for $s=1$ (you probably already know that $L(1,\chi_4)=\pi/4$). The same analysis we used to get an estimate on the Mellin transform of $\pi(\cdot)$ from the Euler product for $\zeta(s)$ can now be used starting from (3) to obtain:[2]

$$s\int_1^\infty \pi(y,\chi_4)y^{-1-s}\,dy = O(1) \qquad (1<s\le 2), \tag{4}$$

where

$$\pi(y,\chi_4) := \pi(y,1 \bmod 4)-\pi(y,3 \bmod 4) = \sum_{p\le y}\chi_4(p).$$

Averaging (4) with (1), we find that

$$\begin{aligned} s\int_1^\infty \pi(y,1 \bmod 4)y^{-1-s}\,dy &= \frac{1}{2}\log\frac{1}{s-1}+O(1) \qquad (1<s\le 2),\\ s\int_1^\infty \pi(y,3 \bmod 4)y^{-1-s}\,dy &= \frac{1}{2}\log\frac{1}{s-1}+O(1) \qquad (1<s\le 2). \end{aligned}$$

This is consistent with $\pi(x,\pm 1 \bmod 4)\sim \frac{1}{2}x/\log x$, and corroborates our expectation that there should be on the average as many primes congruent to $+1 \bmod 4$ as $-1 \bmod 4$. Specifically, it shows that for $a=\pm 1$ the set of primes congruent to $a \bmod 4$ has logarithmic density $1/2$ in the primes. This concept is defined as follows:

Definition. Suppose P is a set of positive integers such that $\sum_{n\in P}1/n$ diverges. A subset S of P is said to have *logarithmic density* δ if

$$\Big(\sum_{n\in S}n^{-s}\Big)\Big/\Big(\sum_{n\in P}n^{-s}\Big)\to\delta$$

as $s\to 1+$. Taking for P the set of primes, we see that a set S of primes has logarithmic density δ if and only if

$$\sum_{p\in S}p^{-s}\sim\delta\log\frac{1}{s-1}$$

as $s\to 1+$.

This notion of "logarithmic density" has the properties we would expect from a density: $\delta\in[0,1]$; a set of positive density is nonempty; if disjoint sets P_1,P_2

[2] Again, the choice of $s_0>1$ does not matter, because we are concerned with the behavior near $s=1$; thus we have made the traditional and convenient choice $s_0=2$, rather than continue with an unspecified s_0 and a distracting subscript in O_{s_0}.

have logarithmic densities δ_1, δ_2, then $P_1 \cup P_2$ has logarithmic density $\delta_1 + \delta_2$; and if P_1, P_2 are sets of logarithmic densities δ_1, δ_2 and $P_1 \subseteq P_2$, then $\delta_1 \leq \delta_2$. See the first Exercise for further information.

We can use the notion of logarithmic density to state Dirichlet's theorem as follows:

Theorem [Dirichlet]**.** *For any positive integer q, and any integer a coprime to q, the primes congruent to $a \bmod q$ constitute a set of logarithmic density $1/\varphi(q)$ in the primes.*

Here φ is the Euler phi ("totient") function, $\varphi(q) = |(\mathbf{Z}/q\mathbf{Z})^*|$. We have just proved the cases $(q, a) = (4, \pm 1)$ of Dirichlet's theorem. The same method disposes of $(q, a) = (3, \pm 1)$, using

$$(1 - 3^{-s})\zeta(s) = 1 + 2^{-s} + 4^{-s} + 5^{-s} + 7^{-s} + 8^{-s} + \cdots$$

and

$$L(s, \chi_3) := 1 - \frac{1}{2^s} + \frac{1}{4^s} - \frac{1}{5^s} + - \cdots = \sum_{n=1}^{\infty} \chi_3(n) n^{-s},$$

Where χ_3 is the multiplicative function defined by

$$\chi_3(n) = \begin{cases} +1, & \text{if } n \equiv +1 \bmod 3; \\ -1, & \text{if } n \equiv -1 \bmod 3; \\ 0, & \text{if } 3|n. \end{cases}$$

With a tad more work we can deal with $q = 8$. Let $\chi_8(n)$ be $+1$ if $n \equiv \pm 1 \bmod 8$, -1 if $n \equiv \pm 3 \bmod 8$, and 0 if n is even. This is a multiplicative function, as is $\chi_4\chi_8$; the resulting L-functions

$$\begin{aligned} L(s, \chi_8) &= \sum_{n=1}^{\infty} \chi_8(n) n^{-s} = 1 - \frac{1}{3^s} - \frac{1}{5^s} + \frac{1}{7^s} + - - + \cdots, \\ L(s, \chi_4\chi_8) &= \sum_{n=1}^{\infty} \chi_4\chi_8(n) n^{-s} = 1 + \frac{1}{3^s} - \frac{1}{5^s} - \frac{1}{7^s} + + - - \cdots \end{aligned}$$

have Euler products for $s > 1$ and are positive for $s > 0$ (to prove this for $L(s, \chi_8)$, group the terms in fours rather than pairs and use the convexity of the function $n \mapsto n^{-s}$). We deduce that

$$\sum_p \chi_8(p) p^{-s} = O(1) \quad \text{and} \quad \sum_p \chi_4\chi_8(p) p^{-s} = O(1)$$

for $s \in (1, 2]$, which combined with previous results yields Dirichlet's theorem for $q = 8$. Similarly we can handle $q = 12$, and with some more effort even $q = 24$.

What about $q = 5$? We have the "quadratic character", which takes n to $+1$ or -1 if $x \equiv \pm 1$ or $\pm 2 \bmod 5$ (and to 0 if $5|n$), but this only lets us separate quadratic from non-quadratic residues mod 5. We need a new idea to

get at the individual nonzero residue classes mod 5. (Recall that $\{5k+2\}$ and $\{5k-2\}$ are the first cases of arithmetic progressions that we could not prove contain infinitely many primes using variations of Euclid's proof.) Let χ be the multiplicative function from $\mathbf{Z}$ to the *complex* numbers which takes $n \equiv 0, 1, 2, 3, 4 \bmod 5$ to $0, 1, i, -i, -1$. Another such function is the complex conjugate $\overline{\chi} = \chi^3$, while χ^2 is the quadratic character and χ^4 is the "trivial character" taking n to 0 or 1 according as $5|n$ or not. The resulting L-functions $\sum_n \chi(n)n^{-s}$, $\sum_n \overline{\chi}(n)n^{-s}$ then take complex values, but still have Euler products and extend to continuous functions on $s > 0$. Moreover, these functions never vanish on $s > 0$; indeed their real and imaginary parts are both nonzero, as we see by combining the real terms into $(5k+1, 5k+4)$ pairs and the imaginary terms into $(5k+2, 5k+3)$ pairs. Likewise the L-function associated to the quadratic character χ^2 has an Euler product and is positive for $s > 0$ by convexity of n^{-s}. We conclude as before that $\sum_p \chi^j(p)p^{-s} = O(1)$ as $s \to 1+$ for each $j = 1, 2, 3$, and recover Dirichlet's theorem for $q = 5$ by taking linear combinations of these sums and $\sum_p p^{-s} = \log \frac{1}{s-1} + O(1)$.

For general q, we proceed analogously, using linear combinations of *Dirichlet characters*, whose definition follows.

Definition. For a positive integer q, a Dirichlet character mod q is a function $\chi : \mathbf{Z} \to \mathbf{C}$ that is

- q-periodic: $n \equiv n' \bmod q \Rightarrow \chi(n) = \chi(n')$;
- supported on the integers coprime to q and on no smaller subset of $\mathbf{Z}$: $(n, q) = 1 \Leftrightarrow \chi(n) \neq 0$; and
- multiplicative: $\chi(m)\chi(n) = \chi(mn)$ for all integers m, n.

To such a character is associated the *Dirichlet L-series*

$$L(s, \chi) := \sum_{n=1}^{\infty} \chi(n)n^{-s} = \prod_p \frac{1}{1 - \chi(p)p^{-s}} \qquad (s > 1). \tag{5}$$

Examples: The *trivial character* χ_0 mod q is defined by $\chi(n) = 1$ if $(n, q) = 1$ and $\chi(n) = 0$ otherwise. Its associated L-series is

$$L(s, \chi_0) = \prod_{p|q} (1 - p^{-s}) \cdot \zeta(s). \tag{6}$$

If l is prime then the *Legendre symbol* $(\cdot/l)$, defined by $(n/l) = 0, 1, -1$ according as n is zero, a nonzero square, or not a square mod l, is a character mod l. If χ is a Dirichlet character mod q then so is its complex conjugate $\overline{\chi}$ (defined of course by $\overline{\chi}(n) = \overline{\chi(n)}$), with $L(s, \overline{\chi}) = \overline{L(s, \chi)}$ for $s > 1$. If χ, χ' are characters mod q, q' then $\chi\chi'$ is a character mod $\mathrm{lcm}(q, q')$. In particular, we have:

Lemma: *For each q, the characters mod q constitute a group under pointwise multiplication, with identity χ_0 and inverse $\chi^{-1} = \overline{\chi}$.* $\square$

What is this group? A Dirichlet character mod q is just a homomorphism from $(\mathbf{Z}/q\mathbf{Z})^*$ to the unit circle, extended by zero to a function on $\mathbf{Z}/q\mathbf{Z}$ and lifted to $\mathbf{Z}$. Therefore the group of such characters is the *Pontrjagin dual* of $(\mathbf{Z}/q\mathbf{Z})^*$. Pontrjagin duality for *finite* abelian groups like $(\mathbf{Z}/q\mathbf{Z})^*$ is easy, since it is equivalent to the theory of the discrete Fourier transform. We next recall the basic facts.

For any finite abelian group G, let $\hat{G}$ be its Pontrjagin dual, defined as the group of homomorphisms from G to the unit circle in $\mathbf{C}$. Then the dual of $G \times H$ is $\hat{G} \times \hat{H}$, and the dual of $\mathbf{Z}/m\mathbf{Z}$ is a cyclic group of order m. Since any finite abelian group is a product of cyclic groups, it follows that $\hat{G}$ is isomorphic with G. This isomorphism is not in general canonical,[3] but there is a canonical isomorphism from G to the dual of $\hat{G}$ (the second dual of G), namely the map taking any $g \in G$ to the homomorphism $\chi \mapsto \chi(g)$. That this is an isomorphism can be checked directly for cyclic groups, and then deduced for any finite abelian G because all such G are direct sums of cyclic groups.

The characters of G are *orthogonal*:

$$\sum_{g \in G} \chi_1(g)\,\overline{\chi_2(g)} = \begin{cases} |G|, & \text{if } \chi_1 = \chi_2; \\ 0, & \text{if } \chi_1 \neq \chi_2. \end{cases}$$

In particular, they are linearly independent, and since there are $|G|$ of them, they form a basis for the vector space of complex-valued functions on G. The decomposition of an arbitrary such function $f : G \to \mathbf{C}$ as a linear combination of characters is achieved by the *inverse Fourier transform*:

$$f = \sum_{\chi \in \hat{G}} f_\chi \chi, \quad \text{where} \quad f_\chi := \frac{1}{|G|} \sum_{g \in G} \overline{\chi}(g) f(g).$$

In particular, the characteristic function of any $g_0 \in G$ is $|G|^{-1} \sum_\chi \overline{\chi}(g_0)\chi$.

What does all this tell us about Dirichlet L-functions and the distribution of primes mod q? First, that if we define $\pi(\cdot, \chi)$ by

$$\pi(x, \chi) := \sum_{a \bmod q} \chi(a)\pi(x, a \bmod q) = \sum_{p < x} \chi(p)$$

then, for all a coprime to q,

$$\pi(x, a \bmod q) = \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi}(a)\pi(x, \chi).$$

Second, that

$$s \int_1^\infty \pi(y, \chi) y^{-1-s}\, dy = \sum_p \chi(p) p^{-s} = \log L(s, \chi) + O(1) \tag{7}$$

[3] For instance, if G is cyclic of order 5, there can be no canonical nondegenerate pairing $\langle \cdot, \cdot \rangle : G \times G \to \mathbf{C}^*$, because such a pairing would have to be invariant under $\mathrm{Aut}(G) = (\mathbf{Z}/5)^*$, but $\langle g^2, g^2 \rangle = \langle g, g \rangle^4 \neq \langle g, g \rangle$.

for $1 < s \le 2$. This is again obtained by taking logarithms in the Euler product (5). The Euler product shows that $L(s,\chi) \neq 0$ for $s > 1$; if χ is complex, "$\log L(s,\chi)$" means the branch of the logarithm that approaches 0 as $s \to \infty$.

For the behavior of $L(s,\chi)$ near $s = 1$, we have:

Lemma. *i) If $\chi = \chi_0$ then $\log L(s,\chi) = \log(1/(s-1)) + O(1)$ as $s \to 1+$.*
ii) For nontrivial χ, the sum defining $L(s,\chi)$ converges for $s > 0$ and defines a continuous function on the positive reals.

Proof: (i) follows from (6), together with our estimate on $\zeta(s)$ for $s \to 1+$. As for (ii), as a special case of character orthogonality we have $\sum_{a \bmod q} \chi(a) = 0$, so $S_\chi(x) := \sum_{0<n\le x} \chi(n)$ is a bounded function of x. Hence (for large $M, N \notin \mathbf{Z}$)[4]

$$\sum_{M<n<N} \frac{\chi(n)}{n^s} = \int_M^N y^{-s}\, dS_\chi(y) = S_\chi(y) y^{-s}\Big|_M^N + s\int_M^N y^{-1-s} S_\chi(y)\, dy$$
$$\ll_\chi M^{-s} + N^{-s},$$

which for fixed $s > 0$ tends to zero as $M, N \to \infty$. Thus the sum $\sum_{n=1}^\infty \chi(n) n^{-s}$ converges. Moreover, for any $s_0 > 0$, the convergence is uniform in $s \ge s_0$. Hence $\sum_{n=1}^\infty \chi(n) n^{-s}$ is the uniform limit of continuous functions $\sum_{n=1}^N \chi(n) n^{-s}$, and is therefore a continuous function on $(0,\infty)$, as claimed. $\square$

From (7) we see that the crucial question is whether $L(1,\chi)$ is nonzero for $\chi \neq \chi_0$: the right-hand side is $O(1)$ if $L(1,\chi) \neq 0$ but $\le -\log(1/(s-1)) + O(1)$ if $L(1,\chi) = 0$ (since $L(s,\chi)$ is differentiable at $s = 1$). Our experience with small q, and our expectation that the primes should not favor one congruence class in $(\mathbf{Z}/q\mathbf{Z})^*$ over another, both suggest that $L(1,\chi)$ will not vanish. This is true, and can be checked in any given case by a finite computation; but our methods thus far do not let us prove it in general (try doing it for $\chi = (\cdot/67)$ or $(\cdot/163)$!). For the time being, then, we can obtain only a conditional result:

Proposition. *Assume that $L(1,\chi) \neq 0$ for all nontrivial characters $\chi \bmod q$. Then Dirichlet's theorem holds for all arithmetic progressions mod q.*

Proof: For each $a \in (\mathbf{Z}/q\mathbf{Z})^*$, multiply (7) by $\overline{\chi}(a)$, and average over χ to obtain

$$\sum_{p \equiv a \bmod q} p^{-s} = \frac{1}{\varphi(q)} \sum_\chi \overline{\chi}(a) \log L(s,\chi) + O(1) = \frac{1}{\varphi(q)} \log \frac{1}{s-1} + O(1)$$

for $1 < s \le 2$, since χ_0 contributes $\chi_0(a) \log \zeta(s) + O(1) = \log \frac{1}{s-1} + O(1)$ to the sum, while the other terms remain bounded by hypothesis. Thus the primes congruent to a mod q have logarithmic density $1/\varphi(q)$, as claimed.

In fact the nonvanishing of $L(1,\chi)$ was proved by Dirichlet, who thus established his celebrated theorem on primes in arithmetic progressions. At least three

[4] We require that $M, N \notin \mathbf{Z}$ to avoid the distraction of whether the Riemann-Stieltjes integral $\int_M^N y^{-s}\, dS_\chi(y)$ includes the terms with $n = M$ or $n = N$ in the sum.

proofs are now known. These three proofs all start with the product of the L-functions associated to all $\varphi(q)$ Dirichlet characters mod q:

$$\prod_{\chi \bmod q} L(s,\chi) = \prod_p \left(\prod_{\chi \bmod q} (1-\chi(p)p^{-s}) \right)^{-1}.$$

The inner product can be evaluated with the following cyclotomic identity:

Let G be a finite abelian group and $g \in G$ an element of order m. Then

$$\prod_{\chi \in \hat{G}} (1-\chi(g)z) = (1-z^m)^{|G|/m} \tag{8}$$

hold identically for all z.

The identity is an easy consequence of the factorization of $1-z^m$ together with the fact that any character of a subgroup $H \subseteq G$ extends in $[G:H]$ ways to a character of G (in our case H will be the cyclic subgroup generated by g).

Let m_p, then, be the multiplicative order of p mod q (for all but the finitely many primes p dividing q). Then we get

$$\prod_{\chi \bmod q} L(s,\chi) = \prod_{p \nmid q} (1-p^{-m_p s})^{-\varphi(q)/m_p}. \tag{9}$$

The left-hand side contains the factor $L(s,\chi_0)$, which is $C/(s-1)+O(1)$ as $s \to 1+$ for some $C > 0$ [in fact $C = \varphi(q)/q$]. Since the remaining factors are differentiable at $s=1$, if any of them were to vanish there the product would remain bounded as $s \to 1+$. So we must show that this cannot happen.

Dirichlet's original approach was to observe that (9) is, up to a few factors $1-p^{-ms}$ with $p|q$, the "zeta function of the cyclotomic number field $\mathbf{Q}(e^{2\pi i/q})$". He then proved that the zeta function $\zeta_K(s)$ of *any* number field K is $\sim C/(s-1)$ as $s \to 1+$ for some positive constant C (and gave an exact formula for C, which includes the class number of K and is thus called the "Dirichlet class number formula"). That is undoubtedly the best way to go about it — but it requires more algebraic number theory than I want to assume here. Fortunately there are at least two ad-hoc simplifications available.

The first is that we need only worry about real characters. If $L(1,\chi) = 0$ then also $L(1,\overline{\chi}) = 0$. Hence if $\chi \neq \overline{\chi}$ but $L(1,\chi) = 0$ then there are at least *two* factors in the left-hand side of (9) that vanish at $s=1$; since they are differentiable there, the product would not only be bounded as $s \to 1+$, but approach zero there — which is impossible because the right-hand side is > 1 for all $s > 1$. But if χ is a real character then $L(s,\chi_0)L(s,\chi)$ is (again within a few factors $1-n^{-s}$ of) the L-function of a quadratic number field. Developing the algebraic number theory of quadratic number fields takes considerably less work than is needed for the full Dirichlet class number formula, and if we only want to get unboundedness as $s \to 1+$ it is even easier — for instance, if $\chi(-1) = -1$

then the right-hand side of (9) is dominated by the zeta function of a binary quadratic form, which is easily seen to be $\gg 1/(s-1)$. However, even this easier proof is beyond the scope of what I want to assume or fully develop in this class.

Fortunately there is a way to circumvent any ζ_K beyond $K = \mathbf{Q}$, using the fact that the right-hand side of (9) also dominates the series $\zeta(\varphi(q) \cdot s)$, which diverges not at $s = 1$ but at $s = 1/\varphi(q)$. Since this s is still positive, we can still get a proof of $L(1, \chi) \neq 0$ from it, but only by appealing to the magic of complex analysis. We thus defer the proof until we have considered $\zeta(s)$ and more generally $L(s, \chi)$ as functions of a *complex* variable s, which we shall have to do anyway to obtain the Prime Number Theorem and results on the density (not just logarithmic density) of primes in arithmetic progressions.

Remarks

Pontrjagin duals. The general setting for Pontrjagin duality is a locally compact abelian topological group G. The Pontrjagin dual of such G is the group $\hat{G}$ of *continuous* homomorphisms from G to the unit circle in $\mathbf{C}$. (When G is finite, or more generally when G is discrete, continuity is automatic.) It is still true, but much harder to prove, that $\hat{G}$ is itself locally compact and that the natural map from G to the Pontrjagin dual of $\hat{G}$ is an isomorphism. The two most familiar examples of a pair of Pontrjagin-dual groups are $G = \hat{G} = \mathbf{R}$ and $\{G, \hat{G}\} = \{\mathbf{R}/\mathbf{Z}, \mathbf{Z}\}$, where in both cases $y \in \hat{G}$ corresponds to the homomorphism $x \mapsto e^{2\pi i x y}$. Two further examples are $G = \hat{G} = \mathbf{Q}_p$ (the p-adic rationals, for some prime p), and $\{G, \hat{G}\} = \{\mathbf{Q}_p/\mathbf{Z}_p, \mathbf{Z}_p\}$, using the homomorphisms $x \mapsto \exp(2\pi i \widetilde{xy})$ where $\widetilde{xy}$ is any rational number of the form $p^\alpha z$ $(\alpha, z \in \mathbf{Z})$ that is congruent to xy mod 1.

As in the discrete case, Pontrjagin duality is used to write functions $f : G \to \mathbf{C}$ as linear combinations of elements of $\hat{G}$, though in general one must replace finite sums by integrals with respect to Haar measure and place some integrability conditions on f, which leads to a much subtler and richer theory. For $G = \hat{G} = \mathbf{R}$ and $\{G, \hat{G}\} = \{\mathbf{R}/\mathbf{Z}, \mathbf{Z}\}$, this theory specializes to the study of the Fourier transform and Fourier series respectively. We shall use Fourier transforms and series several times in the sequel. Fourier analysis on p-adic numbers will not concern us here, but is an important tool in Tate's generalization of properties of $\zeta(s)$ and $L(s, \chi)$ to zeta and L functions of number fields.

Zeta functions of number fields. Let K be any number field (finite algebraic extension of $\mathbf{Q}$), and O_K its ring of algebraic integers. The "zeta function" $\zeta_K(s)$ is $\sum_I |I|^{-s}$, where I ranges over nonzero ideals of O_K and $|I| = [O_K : I]$ is the norm of I. For instance, $\zeta(s) = \zeta_{\mathbf{Q}}(s)$, and if $K = \mathbf{Q}[i]$ then $\zeta_K(s) = \frac{1}{4}\sum(m^2 + n^2)^{-s}$, the sum extending over all $(m, n) \in \mathbf{Z}^2$ other than $(0, 0)$. The relation between the product (9) and the zeta function of $\mathbf{Q}(e^{2\pi i/q})$ can be made more precise: if we replace each χ by its underlying primitive character (see the Exercises), the product is exactly the zeta function of that cyclotomic number field. Similarly, for any quadratic field K there is a primitive Dirichlet character χ such that $\zeta_K(s) = \zeta(s)L(s, \chi)$. These are the prototypical examples

of the factorization of a zeta function as a product of Artin L-functions; the fact that the "Artin L-functions" for 1-dimensional representations of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ are Dirichlet series is a prototype for class field theory. Dirichlet's theorem in turn generalizes to the Čebotarev density theorem. These theorems all require more algebraic machinery than the results we shall obtain using only the Riemann zeta function and Dirichlet L-functions, but much the same analytic methods. Therefore we shall not develop them further in Math 229.

Exercises

Concerning density:

1. If P is an infinite set of integers, the *(natural) density* of any subset $S \subseteq P$ is

$$\lim_{x\to\infty} \#\{n \in S : n < x\}/\#\{n \in P : n < x\},$$

if the limit exists. Check that this satisfies the same properties we noted for the logarithmic density (density of subsets, disjoint unions, etc.). Show that if $\sum_{n\in P} 1/n$ diverges and $S \subset P$ has density δ in P then it also has logarithmic density δ in P. (Use partial summation to write $\sum_{n\in S} n^{-s}$ as an integral involving $\#\{n \in S : n < x\}$.) If P is the set of natural numbers and S_d $(d = 1, 2, \ldots, 9)$ is the subset consisting of integers whose first decimal digit is d, show that S_d has logarithmic density $\log_{10}(1 + \frac{1}{d})$ in P but no natural density. Does every set of natural numbers have a logarithmic density?

While not every set with a logarithmic density has a natural density, we shall see that the primes congruent to a mod q do have natural density $1/\varphi(q)$ in the primes. As for the sets S_d, their logarithmic densities account for "Benford's Law", the observation that in many naturally occurring "random numbers" the initial digit d occurs with frequency $\log_{10}(1 + \frac{1}{d})$, rather than $1/9$ as one might expect.

Concerning Euler products:

2. One may associate to any sequence $(a_1, a_2, a_3, \ldots)$ of complex numbers a Dirichlet series $L(s) = \sum_{n=1}^{\infty} a_n n^{-s}$, which converges absolutely in some right half-plane $s > s_0$ if $a_n \ll n^{s_0-1}$. Show that $L(s)$ has an Euler product

$$L(s) = \prod_p \left(\sum_{c=0}^{\infty} \frac{a_{p^c}}{p^{cs}} \right)$$

if and only if $a_{mn} = a_m a_n$ for any m, n such that $\gcd(m, n) = 1$. (Such functions $n \mapsto a_n$ are called "multiplicative". Note that necessarily $a_1 = 1$ if $\{a_n\}$ is multiplicative.)

3. Let $f(s)$ be the sum of n^{-s} over squarefree positive integers n. Express $f(s)$ in terms of the zeta function, and evaluate $f(2)$. Given k, what is the coefficient of n^{-s} in the Dirichlet series for $\zeta(s - k)$, or $\zeta(s)\zeta(s - k)$?

4. Find $a_1, a_2, \ldots$ such that $\sum_p p^{-s} = \sum_{n=1}^{\infty} a_n \log \zeta(ns)$ for all $s > 1$. Use this (and a computer package that knows about $\zeta(2n)$ and high-precision arithmetic)

to calculate that

$$\sum_p \frac{1}{p^2} = 0.45224742004106549850654336483224793417323\ldots$$

Note that this is much greater accuracy than we could reasonably expect to reach by summing the series directly. We shall see that this trick can be adapted to efficiently compute $\sum_p f(p)$ for many natural choices of f.

Concerning Pontrjagin duality:

5. Show that to any homomorphism $\alpha : H \to G$ between finite abelian groups there is a canonically associated homomorphism $\hat{\alpha} : \hat{G} \to \hat{H}$ in the opposite direction between their Pontrjagin duals. Check that α is the dual of $\hat{\alpha}$ (under the canonical identification of G and H with the duals of $\hat{G}, \hat{H}$), and that if β is a homomorphism from G to a finite abelian group K then the dual of the composite homomorphism $\beta \circ \alpha : H \to K$ is $\hat{\alpha} \circ \hat{\beta}$. Prove that $\mathrm{im}(\alpha) = \ker(\beta)$ if and only if $\mathrm{im}(\hat{\beta}) = \ker(\hat{\alpha})$.

In particular, if $H \to G$ is an injection, it follows (by taking β to be the quotient map $G \to G/\alpha(H)$) that the restriction map $\hat{\alpha} : \hat{G} \to \hat{H}$ is a surjection; this was used to prove the cyclotomic identity (8). An adherent of the categorical imperative would summarize this exercise, together with the easy observations that $\widehat{\mathrm{id}} = \mathrm{id}$ (when $G = H$) and $\hat{0} = 0$, by saying that Pontrjagin duality is an "exact contravariant functor on the category of finite abelian groups".

Concerning Dirichlet characters:

6. Show that the integers q modulo which all the Dirichlet characters are *real* (take on only the values $0, \pm 1$) are precisely 24 and its factors. Show that every real Dirichlet character is of the form $\chi_0 \psi \prod_{l \in S} (\cdot/l)$, where χ_0 is the trivial character, $\psi = \chi_4^{\epsilon_4} \chi_8^{\epsilon_8}$ for some $\epsilon_4, \epsilon_8 \in \{0, 1\}$, and S is a (possibly empty) finite set S of odd primes.

7. Let χ_0 be the trivial character mod q, and let q_1 be some factor of q. For any character $\chi_1 \bmod q_1$ there is a character $\chi \bmod q$ defined by $\chi = \chi_0 \chi_1$. Express $L(s, \chi)$ in terms of $L(s, \chi_1)$. Conclude that $L(1, \chi) \neq 0$ if and only if $L(1, \chi_1) \neq 0$.

8. A character mod q that cannot be obtained in this way from any character mod a *proper* factor $q_1 | q$ (a factor other than q itself) is called *primitive*. Show that any Dirichlet character χ comes from a unique primitive character χ_1. [The modulus of this χ_1 is called the *conductor* of χ.] Show that the number of primitive characters mod n is $n \prod_{p|n} \alpha_p$, where $\alpha_p = ((p-1)/p)^2$ if $p^2 | n$ and $(p-2)/p$ if $p \| n$. NB there are no primitive characters mod n when $2 \| n$.

The notation $p^f \| n$ means that p^f divides n "exactly"; that is, $p^f | n$ but p^{f+1} does not divide n. Equivalently, the p-valuation of n is f.

9. Deduce the fact that for any q there is at most one nontrivial character χ mod q such that $L(1, \chi) = 0$, as a consequence of (7) together with the fact that $\pi(x, a \bmod q) \geq 0$ for all x, a, q. [In the final analysis, this is not much different

from our proof using the product of L-series.] Using either this approach or the one based on (9), prove that there is at most one *primitive* Dirichlet character of any modulus whose L-function vanishes at $s = 1$. [Assume there were two, and obtain two different imprimitive characters to the same modulus whose L-functions both vanish at $s = 1$, which we've already shown impossible. We shall encounter this trick again when we come to Siegel's ineffective lower bound on $L(1, \chi)$.]

Concerning L-series:

10. Show that if χ is a nontrivial character then $L(s, \chi)$ is infinitely differentiable on $s \in (0, \infty)$, and its m-th derivative is given by the convergent sum $\sum_{n=1}^{\infty} (-\log n)^m \chi(n) n^{-s}$ $(m = 1, 2, 3, \ldots)$.

11. i) Prove that if s has real part $\sigma > 1$ then $\zeta(2\sigma)/\zeta(\sigma) < |L(s, \chi)| \leq \zeta(\sigma)$ for all Dirichlet characters χ.
ii) Prove that these bounds are sharp by showing that for all $\sigma > 1$ and $\epsilon > 0$ there exist infinitely many χ such that $L(\sigma, \chi) > \zeta(\sigma) - \epsilon$ and infinitely many χ such that $L(\sigma, \chi) < \zeta(2\sigma)/\zeta(\sigma) + \epsilon$.

We shall show that analogous bounds are also sharp for individual Dirichlet characters: for each χ, σ, ϵ there exist s of real part σ such that $|L(s, \chi)|$ is arbitrarily close to $\zeta^*(\sigma)$, and s of real part σ such that $|L(s, \chi)|$ is arbitrarily close to $\zeta^*(2\sigma)/\zeta^*(\sigma)$, where the $*$'s indicate removal of the Euler factors at the modulus of χ.

12. [Zeta function of a quadratic form] For some positive integer r, let $Q : \mathbf{R}^r \to \mathbf{R}$ be a positive-definite quadratic form. Show that

$$\zeta_Q(s) := \sum_{\substack{n \in \mathbf{Z}^r \\ n \neq 0}} \frac{1}{Q(n)^s}$$

converges absolutely if and only if s has real part $> r/2$, and determine the limit of $(s - (r/2))\zeta_Q(s)$ as $s \to r/2$ from above. [Use partial summation with respect to $\#\{n \in \mathbf{Z}^r : Q(n) \leq x\}$. Check that your answer is consistent with the answer for $r = 1$, when $Q(n) = an^2$ and $\zeta_Q(s) = a^{-s}\zeta(2s)$.] If Q is the standard quadratic form $Q(n) = n_1^2 + n_2^2$, prove that $\zeta_Q(s) = 4\zeta(s)L(s, \chi_4)$. (This is an example of the relation between (9) and the zeta function of a number field. Check that it is consistent with your formula for the growth of $\zeta_Q(s)$ as $s \to r/2$.) Obtain a similar formula for $Q(n) = n_1^2 + n_1 n_2 + n_2^2$. What other Q can you find for which $\zeta_Q(s)$ is proportional to a product of Dirichlet L-functions?