Math 229: Introduction to Analytic Number Theory

$L(s, \chi)$ as an entire function; Gauss sums

We first give, as promised, the analytic proof of the nonvanishing of $L(1, \chi)$ for a Dirichlet character χ mod q; this will complete our proof of Dirichlet's theorem that there are infinitely primes in the arithmetic progression $\{mq+a : m \in \mathbf{Z}_{>0}\}$ whenever $(a, q) = 1$, and that the logarithmic density of such primes is $1/\varphi(q)$.[1]

We follow [Serre 1973, Ch. VI §2]. Functions such as $\zeta(s)$, $L(s, \chi)$ and their products are special cases of what Serre calls "Dirichlet series": functions

$$f(s) := \sum_{n=1}^{\infty} a_n e^{-\lambda_n s} \tag{1}$$

with $a_n \in \mathbf{C}$ and $0 \leq \lambda_n < \lambda_{n+1} \to \infty$. [For instance, $L(s, \chi)$ is of this form with $\lambda_n = \log n$ and $a_n = \chi(n)$.] We assume that the a_n are small enough that the sum in (1) converges for some $s \in \mathbf{C}$. We are particularly interested in series such as

$$\zeta_q(s) := \prod_{\chi \bmod q} L(s, \chi)$$

whose coefficients a_n are nonnegative. Then if (1) converges at some real σ_0, it converges uniformly on $\sigma \geq \sigma_0$, and $f(s)$ is analytic on $\sigma > \sigma_0$. Thus a series (1) has a maximal open half-plane of convergence (if we agree to regard $\mathbf{C}$ itself as an open half-plane for this purpose), namely $\sigma > \sigma_0$ where σ_0 is the infimum of the real parts of $s \in \mathbf{C}$ at which (1) converges. This σ_0 is then called the "abscissa of convergence"[2] of (1).

We claim that if σ_0 is finite then it is a singularity of f; that is:

Proposition. *Suppose that the series (1) has positive coefficients a_n, and that there exists $\rho \in \mathbf{R}$ such that the series converges in the half-plane $\sigma > \rho$ and extends to an analytic function in a neighborhood of ρ. Then the abscissa of convergence of the series is strictly smaller than ρ.*

Proof: Since $f(s - \rho)$ is again of the form (1) with nonnegative coefficients $e^{\lambda_n \rho} a_n$, it is enough to prove the Proposition for $\rho = 0$. Since f is then analytic in $\sigma > 0$ and also in $|s| < \delta$ for some $\delta > 0$, it is analytic in $|s - 1| \leq 1 + \epsilon$ for sufficiently small ϵ, specifically any $\epsilon < \sqrt{1 + \delta^2} - 1$. Expand f in a Taylor series about $s = 1$. Since (1) converges uniformly in a neighborhood of that point, it may be differentiated termwise, and we find that its m-th derivative there is

$$f^{(m)}(1) = \sum_{n=1}^{\infty} (-\lambda_n)^m a_n e^{-\lambda_n}.$$

[1] Davenport gives a simpler proof of Dirichlet's theorem, also involving L-functions but not yet obtaining even the logarithmic density, in Chapter 4, attributing the basic idea to Landau 1905.

[2] The quaint word "abscissa" for "x-coordinate" is still sometimes encountered in analytic geometry, alongside "ordinate" (a.k.a. "y-coordinate").

Taking $s = -\epsilon$, we obtain the convergent sum

$$f(-\epsilon) = \sum_{m=0}^{\infty} \frac{(-1-\epsilon)^m}{m!} f^{(m)}(1) = \sum_{m=0}^{\infty} \frac{(1+\epsilon)^m}{m!} \left[\sum_{n=1}^{\infty} (+\lambda_n)^m a_n e^{-\lambda_n} \right].$$

Since all the terms in the sum are nonnegative, the sum converges absolutely, and may be summed in any order. Therefore

$$f(-\epsilon) = \sum_{n=1}^{\infty} a_n \left[\sum_{m=0}^{\infty} e^{-\lambda_n} \frac{(1+\epsilon)^m}{m!} \lambda_n^m \right].$$

But the new inner sum is just a Taylor series for $e^{\lambda_n \epsilon}$. So we have shown that the series (1) converges at $s = -\epsilon$, and thus has abscissa of convergence $\sigma_0 \leq -\epsilon < 0 = \rho$. $\square$

We can now prove:

Theorem. *Let χ be a nontrivial character mod q. Then $L(1, \chi) \neq 0$.*

Proof: We know already that $L(s, \chi)$ extends to a function on $\sigma > 0$ that is analytic except for the simple pole of $L(s, \chi_0)$ at $s = 1$. If any $L(s, \chi)$ vanished at $s = 1$ then

$$\zeta_q(s) := \prod_{\chi \bmod q} L(s, \chi)$$

would extend to an analytic function on $\sigma > 0$. But we observed already that $\zeta_q(s)$ is a Dirichlet series $\sum_n a_n n^{-s}$ with nonnegative coefficients that converges at least in $\sigma > 1$. By our Proposition, this series would thus converge in $\sigma > 0$. But we also have $a_n \geq 1$ if $n = k^{\varphi(q)}$ for some k coprime to q. Therefore $\sum_n a_n n^{-\sigma}$ diverges for $\sigma \leq 1/\varphi(q)$. This contradiction proves that no $L(1, \chi)$ vanishes. $\square$

We have thus established Dirichlet's theorem on the infinitude and logarithmic density of primes $qm + a$. But we want more than logarithmic density, namely asymptotics of $\pi(x, a \bmod q)$, or equivalently of $\pi(x, \chi)$. As with the Prime Number Theorem, it will be enough to estimate

$$\psi(x, \chi) := \sum_{n<x} \chi(n) \Lambda(n),$$

for which we have an integral approximation

$$\psi(x, \chi) = \frac{1}{2\pi i} \int_{1+\frac{1}{\log x}-iT}^{1+\frac{1}{\log x}+iT} -\frac{L'}{L}(s, \chi)\, x^s \frac{ds}{s} + O\left(\frac{x \log^2 x}{T}\right) \qquad (T \in [1, x]).$$

We therefore seek a partial-fraction decomposition for L'/L, which in turn leads us to prove an analytic continuation and functional equation for $L(s, \chi)$.

Our key tool in proving the functional equation for $\zeta(s)$ was the Poisson summation formula, which we recovered from the Fourier series of

$$F(x) := \sum_{m=-\infty}^{\infty} f(x+m)$$

by setting $x = 0$. We now need this Fourier series

$$F(x) = \sum_{n=-\infty}^{\infty} \hat{f}(n) e^{-2\pi i n x}$$

for fractional x. (Here $\hat{f}$ is the Fourier transform of f, defined by

$$\hat{f}(y) = \int_{-\infty}^{\infty} e^{2\pi i x y} f(x)\, dx \tag{2}$$

as before.) Let $a \mapsto c(a)$ be any function from $\mathbf{Z}/q\mathbf{Z}$ to $\mathbf{C}$. Then we have

$$\sum_{m=-\infty}^{\infty} c(m) f(m/q) = \sum_{a \bmod q} c(a) F(a/q) = \sum_{n=-\infty}^{\infty} \hat{c}(-n) \hat{f}(n), \tag{3}$$

where $\hat{c}$ is the *discrete Fourier transform* of c, defined by

$$\hat{c}(n) := \sum_{a \bmod q} c(a) e^{2\pi i n a/q}. \tag{4}$$

Now suppose c is a *primitive* character χ mod q. We use the notation τ_n for its discrete Fourier transform; that is,

$$\tau_n(\chi) := \sum_{a \bmod q} \chi(a) e^{2\pi i n a/q}.$$

We claim:

Lemma. *Assume that χ is a primitive character mod q. Then*

$$\tau_n(\chi) = \overline{\chi}(n) \tau_1(\chi) \tag{5}$$

holds for all $n \in \mathbf{Z}$. That is, the discrete Fourier transform of a primitive character χ is $\tau_1(\chi)\overline{\chi}$. If n is coprime to q then (5) holds for all characters χ mod q, primitive or not.

Proof: Let $d = \gcd(n, q)$. If $d = 1$ then we may replace a by $n^{-1}a$, from which $\tau_n(\chi) = \overline{\chi}(n)\tau_1(n)$ follows. If $d > 1$ then $\overline{\chi}(n) = 0$, so we want to show $\tau_n(\chi) = 0$. Let $q_0 = q/d$, and rearrange the $\tau_n(\chi)$ sum according to a mod q_0:

$$\tau_n(\chi) = \sum_{a_0 \bmod q_0} \sum_{\substack{a \bmod q \\ a \equiv a_0 \bmod q_0}} \chi(a) e^{2\pi i n a/q} = \sum_{a_0 \bmod q_0} e^{2\pi i n a_0/q} \left[\sum_{a \equiv a_0 \bmod q_0} \chi(a) \right].$$

We claim that the inner sum vanishes. This is clear unless $\gcd(a_0, q_0) = 1$. In that case the inner sum is

$$\chi(a_1) \sum_{\substack{a \bmod q \\ a \equiv 1 \bmod q_0}} \chi(a),$$

for any $a_1 \equiv a_0 \bmod q_0$. But this last sum is the sum of a character on the group of units mod q congruent to 1 mod q_0, and so vanishes unless that character is trivial — and if $\chi(a) = 1$ whenever $a \equiv 1 \bmod q_0$ then χ comes from a character mod q_0 (why?) and is thus not primitive. This completes the proof. □

We generally abbreviate $\tau_1(\chi)$ as $\tau(\chi)$, and call that number

$$\tau(\chi) := \sum_{a \bmod q} \chi(a) e^{2\pi i a/q} \tag{6}$$

the *Gauss sum* of the character χ. We then have:

Theorem. *Let $f : \mathbf{R} \to \mathbf{C}$ be any function satisfying the hypotheses of Poisson summation. Then for any primitive character $\chi \bmod q$ we have*

$$\sum_{m=-\infty}^{\infty} \chi(m) f(m/q) = \tau(\chi) \sum_{n=-\infty}^{\infty} \overline{\chi}(-n) \hat{f}(n). \tag{7}$$

Proof: Substitute the formula (5) of our Lemma into (3). □

This may be regarded as the "twist by χ" of the Poisson summation formula.

For even characters χ, we know what to do next: take $f(x) = e^{-\pi u (qx)^2}$ in (7), and apply the Mellin transform to the resulting identity. This is actually easier than our proof of the functional equation for $\zeta(s)$, because we do not need to split the integral in two. (Ultimately this is because, unlike $\zeta(\cdot)$, the L-function of a nontrivial primitive character has no poles.) Let[3]

$$\theta_\chi(u) := \sum_{n=-\infty}^{\infty} \chi(n) e^{-\pi n^2 u}.$$

By (7), together with the fact that the Fourier transform of $f(x) = e^{-\pi u (qx)^2}$ is $\hat{f}(y) = u^{-1/2} q^{-1} e^{-\pi u^{-1} (y/q)^2}$, we obtain

$$\theta_\chi(u) = \frac{\tau(\chi)}{q u^{1/2}} \sum_{n=-\infty}^{\infty} \overline{\chi}(-n) e^{-\pi u^{-1} (n/q)^2} = \frac{\tau(\chi)}{q u^{1/2}} \theta_{\overline{\chi}}(1/q^2 u). \tag{8}$$

Note that, unless $q = 1$, it follows that $\theta_\chi(u)$ is rapidly decreasing as $u \to 0+$, because $\chi(0) = 0$. Integrating termwise, we find

$$2\pi^{-s/2} \Gamma(s/2) L(s, \chi) = \int_0^\infty \theta_\chi(u) u^{s/2} \, \frac{du}{u}$$

for $\mathrm{Re}(s) > 1$. Since $\theta_\chi(u) \ll \exp(-\pi/q^2 u)$ as $u \to 0+$, the integral converges for all s, and gives the analytic continuation of $L(s, \chi)$ to an entire function with

[3] Our $\theta_\chi(u)$ is called $\psi(qu, \chi)$ in [Davenport 1967, Ch.9].

zeros at the poles $s = 0, -2, -4, -6, \ldots$ of $\Gamma(s/2)$. Moreover, by (8) the integral is also

$$\frac{\tau(\chi)}{q}\int_0^\infty \theta_{\overline{\chi}}(1/q^2u)u^{(s-1)/2}\,\frac{du}{u} = \frac{\tau(\chi)}{q}\int_0^\infty \theta_{\overline{\chi}}(u)(q^2u)^{(1-s)/2}\,\frac{du}{u}$$

$$= \frac{\tau(\chi)}{q^s}\int_0^\infty \theta_{\overline{\chi}}(u)u^{(1-s)/2}\,\frac{du}{u}.$$

This last integral is $2\tau(\chi)q^{-s}\Gamma(\frac{1}{2}(1-s))\pi^{(s-1)/2}L(1-s,\overline{\chi})$ for $\sigma \in (0,1)$, and thus by analytic continuation for all $s \in \mathbf{C}$. We can write the functional equation symmetrically by setting

$$\xi(s,\chi) := (\pi/q)^{-s/2}\Gamma(s/2)L(s,\chi),$$

which is now an entire function: $\xi(s,\chi)$ is related with $\xi(s,\overline{\chi})$ by

$$\xi(s,\chi) = \frac{\tau(\chi)}{\sqrt{q}}\xi(1-s,\overline{\chi}). \tag{9}$$

What about odd χ? The same definition of θ_χ would yield zero. We already indicated (in the exercises on the functional equation for ζ and ξ) the correct approach: we apply (7) not to the Gaussian $e^{-\pi u(qx)^2}$ but to its derivative, which is proportional to $xe^{-\pi u(qx)^2}$. Using the general fact that the Fourier transform of f' is $-2\pi iy\hat{f}(y)$ (integrate by parts in the definition (2) of $\widehat{f'}$) we see that the Fourier transform of $xe^{-\pi u(qx)^2}$ is $(iy/(u^{1/2}q)^3)e^{-\pi u^{-1}(y/q)^2}$. So, if we define[4]

$$\vartheta_\chi(u) := \sum_{n=-\infty}^{\infty} n\chi(n)e^{-\pi n^2u},$$

we find

$$\vartheta_\chi(u) = \frac{\tau(\chi)}{iq^2u^{3/2}}\vartheta_{\overline{\chi}}(1/q^2u). \tag{10}$$

This time we must multiply ϑ_χ by $u^{(s+1)/2}\,du/u$ to cancel the extra factor of n. We obtain the integral formula

$$2\pi^{-(s+1)/2}\Gamma((s+1)/2)L(s,\chi) = \int_0^\infty \vartheta_\chi(u)u^{(s+1)/2}\,\frac{du}{u}$$

for $L(s,\chi)$. Again (10) together with $\chi(0) = 0$ tells us that $\vartheta_\chi(u)$ vanishes rapidly as $u\to 0+$, and thus that our integral extends to an entire function of s; note however that the resulting trivial zeros of $L(s,\chi)$ are at the negative *odd* integers. The functional equation (10) again gives us a relation between $L(s,\chi)$ and $L(1-s,\overline{\chi})$, which this time has the symmetrical form

$$\xi(s,\chi) = \frac{\tau(\chi)}{i\sqrt{q}}\xi(1-s,\overline{\chi}), \tag{11}$$

[4]Our $\vartheta_\chi(u)$ is Davenport's $\psi_1(qu,\chi)$.

with

$$\xi(s,\chi) := (\pi/q)^{-(s+1)/2}\Gamma((s+1)/2)L(s,\chi).$$

We may combine (9) with (11) by introducing an integer a depending on χ:

$$\mathsf{a} := \begin{cases} 0, & \text{if } \chi(-1) = +1; \\ 1, & \text{if } \chi(-1) = -1. \end{cases}$$

That is, $\mathsf{a} = 0$ or 1 according as χ is even or odd. We then have:

Theorem. *Let χ be any primitive character mod q, and $\mathsf{a} = 0$ or 1 as above. Define*

$$\xi(s,\chi) := (\pi/q)^{-(s+\mathsf{a})/2}\Gamma((s+\mathsf{a})/2)L(s,\chi).$$

Then the ξ functions of χ and $\overline{\chi}$ are related by the functional equation

$$\xi(s,\chi) = \frac{\tau(\chi)}{i^{\mathsf{a}}\sqrt{q}}\xi(1-s,\overline{\chi}). \tag{12}$$

Note that this holds even for the case $q = 1$, in which $L(s,\chi)$ and $\xi(s,\chi)$ reduce to $\zeta(s)$ and $\xi(s)$. In that case, we concluded that $(s^2-s)\xi(s)$ is an entire function of order 1. For $q > 1$, the function $\xi(s,\chi)$ has no poles, and we find in the same way that $\xi(s,\chi)$ is an entire function of order 1. We shall develop its product formula and deduce the asymptotics of $\psi(x,\chi)$ in the next lecture notes.

Meanwhile, we prove some basic results concerning Gauss sums. First we find $|\tau(\chi)|$:

Proposition. *The Gauss sum $\tau(\chi)$ of any primitive Dirichlet character χ mod q has absolute value $q^{1/2}$.*

Proof: We obtain this as a special case of the Parseval identity for discrete Fourier transforms:

$$\sum_{n \bmod q} |\hat{c}(n)|^2 = q \sum_{a \bmod q} |c(a)|^2 \tag{13}$$

for any function $a \mapsto c(a)$ from $\mathbf{Z}/q\mathbf{Z}$ to $\mathbf{C}$. The identity (13) can be proved either directly or by observing that the functions $a \mapsto e^{2\pi ina/q}$ are orthogonal with constant norm q. Now take $c(a) = \chi(a)$. We have seen that $\hat{c}(n) = \tau(\chi)\overline{\chi}(n)$. Therefore (13) becomes $|\tau(\chi)|^2\varphi(q) = q\varphi(q)$, whence $|\tau(\chi)|^2 = q$ as claimed. □

The Gauss sum may be regarded as a discrete analogue of the Gamma integral: the factors x^{s-1} and e^{-x} in the integral $\Gamma(s) = \int_0^\infty x^{s-1}e^{-x}\,dx$ are a varying homomorphism from $\mathbf{R}^*_{>0}$ to $\mathbf{C}^*$ and a fixed homomorphism from the additive group $\mathbf{R}$ to $\mathbf{C}^*$; in the Gauss sum (6), these are replaced by the varying homomorphism χ from $(\mathbf{Z}/q\mathbf{Z})^*$ and the fixed homomorphism $a \mapsto e^{2\pi ia/q}$ from $(\mathbf{Z}/q\mathbf{Z}, +)$. The analogy is particularly close when q is prime, in which case $\mathbf{Z}/q\mathbf{Z}$, like $\mathbf{R}$, is a field. In this case the Beta integral has a corresponding

analogue in the *Jacobi sums*

$$J(\chi,\chi') := \sum_{c \bmod q} \chi(c)\chi'(1-c).$$

We do not require that χ and χ' be primitive. Note that unlike $\tau(\chi)$, which may involve both q-th and $(q-1)$st roots of unity, the Jacobi sum $J(\chi,\chi')$ involves only $(q-1)$st roots. Nevertheless it can be evaluated in terms of Gauss sums:

Proposition. *Let χ,χ' be Dirichlet characters mod q. Then*

$$J(\chi,\chi') = \frac{\tau(\chi)\tau(\chi')}{\tau(\chi\chi')}, \tag{14}$$

provided that none of $\chi,\chi',\chi\chi'$ is the trivial character χ_0. If $\chi=\chi'=\chi_0$ then $J(\chi,\chi')=q-2$; if exactly one of χ and χ' is trivial then $J(\chi,\chi')=-1$; and if χ,χ' are nontrivial but $\chi\chi'=\chi_0$ then $J(\chi,\chi')=-\chi(-1)$.

Proof: It is clear that $J(\chi_0,\chi_0)=q-2$, so we henceforth assume that χ,χ' are not both trivial. As in our evaluation of $\mathrm{B}(s,s')$ in terms of the Gamma function, we consider the double sum

$$\tau(\chi)\tau(\chi') = \sum_{a,a' \bmod q}\sum \chi(a)\chi'(a')e^{2\pi i(a+a')/q}.$$

Let $b=a+a'$. The terms with $b=0$ sum to

$$\chi'(-1)\sum_{a \bmod q}\chi\chi'(a) = \begin{cases}\chi(-1)(q-1), & \text{if } \chi'=\overline{\chi};\\ 0, & \text{otherwise.}\end{cases}$$

To sum the terms for fixed nonzero b, let $a=cb$ and $a'=(1-c)b$ to find

$$e^{2\pi ib/q}\chi\chi'(b)\sum_{c \bmod q}\chi(c)\chi'(1-c) = e^{2\pi ib/q}\chi\chi'(b)J(\chi,\chi'). \tag{15}$$

Hence if $\chi\chi'=\chi_0$ (that is, if $\chi'=\overline{\chi}$), we have

$$\tau(\chi)\tau(\chi') = \chi(-1)(q-1) - J(\chi,\chi').$$

But

$$\tau(\overline{\chi}) = \sum_{a \bmod q}\overline{\chi}(a)e^{2\pi ia/q} = \overline{\sum_{a \bmod q}\chi(a)e^{-2\pi ia/q}} = \chi(-1)\overline{\tau(\chi)}, \tag{16}$$

so

$$J(\chi,\overline{\chi}) = \chi(-1)(q-1) - \tau(\chi)\tau(\chi') = \chi(-1)(q-1-|\tau(\chi)|^2) = -\chi(-1).$$

(We could also have obtained this directly from $\chi(c)\overline{\chi}(1-c)=\overline{\chi}(c^{-1}-1)$, which in turn yields an alternative proof of $|\tau(\chi)|=q^{1/2}$ in the prime case.) Otherwise (15) yields (14). □

Corollary. *The Jacobi sum $J(\chi, \chi')$ has absolute value $q^{1/2}$ if each of $\chi, \chi', \chi\chi'$ is nontrivial.*

The formula (14) is the beginning of a long and intricate chapter of the arithmetic of cyclotomic number fields; it can also be used to count solutions of certain Diophantine equations mod q, showing for instance that if $q \equiv 1 \bmod 3$ then there are $q/9 + O(\sqrt{q})$ values of $c \neq 0, 1$ in $\mathbf{Z}/q\mathbf{Z}$ such that both c and $1 - c$ are cubes. See the Exercises for more details and examples.

Remarks

Our extended Poisson identity (3) also has a generalization to locally compact abelian groups. Let G be such a group, H a closed subgroup, and K a closed subgroup of H. Then the annihilators $H^\perp, K^\perp$ in $\hat{G}$ are closed subgroups, with $H^\perp \subseteq K^\perp$. Moreover, $K^\perp/H^\perp$ is canonically identified with the Pontrjagin dual of H/K. Then one can choose Haar measures on G, H, H/K, and $K^\perp$ such that

$$\int_{x \in H} c(x + K) f(x) = \int_{y \in K^\perp} \hat{c}(-y + H^\perp) \hat{f}(y).$$

under suitable hypothesis on the functions $c : H/K \to \mathbf{C}$ and $f : H \to \mathbf{C}$. The formula (3) is the special case $G = \hat{G} = \mathbf{R}$, $K = K^\perp = \mathbf{Z}$, $H = q^{-1}\mathbf{Z}$, $H^\perp = q\mathbf{Z}$.

The formula for $\xi(s, \chi)$, and the distinction between even and odd characters χ, can be interpreted structurally as follows. Let χ be a primitive character mod q. We mentioned already that $L(s, \chi)$ is a factor in a product formula for $\zeta_K(s)$, the zeta function of the cyclotomic number field $K = \mathbf{Q}(e^{2\pi i/q})$; and that for any number field K, the Euler product for ζ_K can be "completed" to a function $\xi_K(s)$ that satisfies a functional equation $\xi_K(s) = \xi_K(1 - s)$. The additional factors come from the discriminant and the archimedean valuations of K. When K is cyclotomic, we can also give such an interpretation of $\xi(s, \chi)$. We may regard χ as a character of $(\mathbf{Z}/q\mathbf{Z})^*$, a group canonically isomorphic with the Galois group $G = \mathrm{Gal}(K/\mathbf{Q})$. For each prime $p \nmid q$, the number $\chi(p)$ that appears in the local factor $(1 - \chi(p)p^{-s})^{-1}$ is then the image under χ of the p-Frobenius element in G. That is, this factor records the p-adic behavior of the Galois extension $K/\mathbf{Q}$. Just as the factor $\Gamma(s/2)$ in $\xi(s) = \xi_{\mathbf{Q}}(s)$ was regarded as a local factor at the archimedean place of $\mathbf{Q}$, the factor $\Gamma((s + \mathsf{a})/2)$ in $\xi(s, \chi)$ can be regarded as an archimedean local factor. Instead of Frobenius, the archimedean place is associated with *complex conjugation*, whose image in $\mathrm{Gal}(K/\mathbf{Q})$ is identified with $-1 \in (\mathbf{Z}/q\mathbf{Z})^*$ under the isomorphism from $(\mathbf{Z}/q\mathbf{Z})$ to G. The factor $\Gamma((s+\mathsf{a})/2)$, which depends on $\chi(-1)$, thus records the image under χ of complex conjugation.

The identity $|\tau(\chi)|^2 = q$ could also have been obtained indirectly from the twisted Poisson formula (7). If f is a function such that both $f, \hat{f}$ satisfy the Poisson hypotheses, we may apply (7) twice to find that either

$$\tau(\chi)\tau(\overline{\chi}) = \chi(-1)q \tag{17}$$

or $\sum_{m \in \mathbf{Z}} \chi(m) f(m/q) = 0$. Since the latter possibility cannot hold for all f

(for instance, consider $f(x) = \exp(-C(x-1/q)^2)$ for large C), we have deduced (17). But (17) is equivalent to $|\tau(\chi)|^2 = q$ by the formula (16) which relates $\tau(\chi)$ and $\tau(\overline{\chi})$.

Exercises

On general Dirichlet series:

1. Suppose the λ_n are closed under addition.
i) Show that for any right half-plane $H = \{s \in \mathbf{C} : \mathrm{Re}(s) \geq \sigma_0\}$ or $H = \{s \in \mathbf{C} : \mathrm{Re}(s) > \sigma_0\}$ the space of Dirichlet series (1) that converge absolutely in H is closed under multiplication. (We allow $\sigma = -\infty$, in which case $H = \mathbf{C}$, as well as $\sigma = +\infty$, in which case we are dealing with formal Dirichlet series.)
ii) If $f(s) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$ and $g(s) = \sum_{n=1}^{\infty} b_n e^{-\lambda_n s}$ are two such functions then the sequence of coefficients of $fg(s)$ is the *convolution* $a*b$ of the sequences a_n, b_n. Prove that convolution is associative: $(a*b)*c = a*(b*c)$. [NB: While this is suggested by part (i), it is not quite an immediate consequence, unless you exclude formal Dirichlet series and show that two Dirichlet series that are equal on H have the same coefficients.] Note that when $\lambda_n = n\lambda_1$ this recovers the usual (additive) convolution $(a*b)_n = \sum_{j+k=n} a_j b_k$.
iii) When $\lambda_n = \log n$, we have $(a*b)_n = \sum_{jk=n} a_j b_k$. Show that the result of part (ii) includes *Möbius inversion*: if $c_n = \sum_{d|n} a_d$ then $a_n = \sum_{d|n} \mu(n/d) c_d$.

2. Consider a Dirichlet series (1) in which a_n need not be positive reals. Clearly this series still has an abscissa of absolute convergence. Less obvious, but still true, is that it also has an abscissa of ordinary convergence. Show that if the sum (1) converges in the usual sense of $\lim_{N\to\infty} \sum_1^N$ at some s_0 then it converges also in $\sigma \geq \mathrm{Re}(s_0)$, the convergence being uniform in $\arg(s - s_0) \leq \alpha$ for each $\alpha < \pi/2$. Deduce that (1) defines an analytic function on $\sigma > \mathrm{Re}(s_0)$. Must the sum converge for all s with $\mathrm{Re}(s) = \mathrm{Re}(s_0)$?

[Since $f(s - s_0)$ is again of the form (1), it is enough to prove this claim for $s_0 = 0$. Assume then that $\sum_{n=1}^{\infty} a_n$ converges, and let $A(x) = -\sum_{\lambda_n > x} a_n$; by hypothesis $A(x) \to 0$ as $x \to \infty$. For large M, N with $M \leq N$, write

$$\sum_{n=M}^{N} a_n e^{-\lambda_n s} = \int_{\lambda_M}^{\lambda_N} e^{-\lambda s}\, dA(\lambda),$$

etc. This is equivalent to the route taken by Serre, but probably more transparent to us. Note that the convergence of the Dirichlet series for $L(s, \chi)$ on $\sigma > 0$ now follows automatically from its convergence for positive real s.]

3. Are the Dirichlet series (1) that converge (but might not converge absolutely) on a given right half-plane H closed under multiplication? (Hint: use the method of the previous Exercise to show that any such Dirichlet series f satisfies $f(s) \ll 1 + |s|$ on H.)

On L-functions:

4. Complete the missing steps in the proof of (11).

5. Suppose χ is a real character. Then (12) relates $\xi(s,\chi)$ with $\xi(s,1-\chi)$. Deduce that $L(s,\chi)$ has a zero of even or odd multiplicity at $s=1/2$ according as $\tau(\chi)=+i^{\mathfrak{a}}\sqrt{q}$ or $\tau(\chi)=-i^{\mathfrak{a}}\sqrt{q}$. In particular, in the minus case $L(1/2,\chi)=0$.

But it is known that in fact the minus case never occurs:

$$\tau(\chi)=+i^{\,\mathfrak{a}}\sqrt{q} \tag{18}$$

holds for all primitive real χ mod q. This was first proved by Gauss after much work. (Davenport proves this in the special case of prime q in Chapter 2, using a later method of Dirichlet that relies on Poisson summation; we outline another proof in the next few Exercises.) It follows that the order of vanishing of $L(s,\chi)$ at $s=1/2$ is even; it is conjectured, but not proved, that in fact $L(1/2,\chi)>0$ for all Dirichlet characters χ. More complicated number fields are known whose zeta functions do vanish (always to even order) at $s=1/2$.

On Gauss sums:

6. Suppose χ is a character mod $q=q_1q_2$ with q_1,q_2 coprime. Then $\chi=\chi_1\chi_2$ for some characters χ_i mod q_i, and χ is primitive if and only if both χ_1 and χ_2 are primitive. (You have shown this in the course of enumerating primitive characters.) In this case, express $\tau(\chi)$ in terms of the q_i, χ_i, and $\tau(\chi_i)$.

7. Suppose further that χ is a real character. Then the same is true of χ_1 and χ_2 (why?). Use your result in the previous Exercise, together with Quadratic Reciprocity, to verify that (18) holds for χ if it holds for each of χ_1 and χ_2. (In the opposite direction, if one proves in some other way that (18) holds for all primitive real Dirichlet characters then one can deduce Quadratic Reciprocity.) Conclude that (18) holds for all real characters if it holds for real characters mod q where q is either 4, 8, or an odd prime. Verify the three cases of even q, and show that if χ is the primitive real character modulo an odd prime q then

$$\tau(\chi)=\sum_{n \bmod q} e^{2\pi i n^2/q}. \tag{19}$$

8. Observe that $\sum_{n \bmod q} e^{2\pi i n^2/q}$ is the trace of the operator $T:\mathbf{C}^q\to\mathbf{C}^q$ that takes a complex-valued function c on $\mathbf{Z}/q\mathbf{Z}$ to its discrete Fourier transform $\hat{c}$. Show that $\hat{\hat{c}}(a)=q\,c(-a)$, and thus that each of the q eigenvalues λ of T is one of $\pm q^{1/2}$ or $\pm iq^{1/2}$. Thus we can evaluate $\tau(q)=\sum_\lambda \lambda$ by determining the multiplicity of each of these four eigenvalues. We already know that $\tau(\chi)=\pm q^{1/2}$ or $\pm iq^{1/2}$ according as $q\equiv 1$ or -1 mod 4. Check that this reduces the determination of $\tau(\chi)$ to computing $\det T$. Compute this determinant (Hint: T is represented by a Vandermonde matrix, and only the phase of $\det T$ is at issue because $|\det T|=\prod_\lambda|\lambda|=q^{q/2}$) to complete the proof of the formula (18) for the sign of $\tau(\chi)$.

The trace description of the sum in (19) does not depend on the primality of q, and yields $N^{-1/2}\sum_{n \bmod N} e^{2\pi i n^2/N}\in\mathbf{Z}[i]$ for all integers $N\geq 1$. It is known that in fact

$$N^{-1/2}\sum_{n \bmod N} e^{2\pi i n^2/N}=\frac{1+(-i)^N}{1-i};$$

that is, $1+i$, 1, 0, or i according as $N \equiv 0$, 1, 2 or 3 mod 4.

9. Recall that the duplication formula for the Gamma function can be obtained by applying the change of variable $u = (1-2x)^2$ to the integral defining $\mathrm{B}(s,s)$. Can you find a τ analog of this identity?

On Jacobi sums:

10. For characters $\chi_1, \ldots, \chi_n$ modulo a prime q, define the generalized Jacobi sum $J(\chi_1, \ldots, \chi_n)$ by

$$J(\chi_1, \ldots, \chi_n) := \sum \cdots \sum \chi_1(a_1) \cdots \chi_n(a_n),$$

where the sum extends over all $(a_1, \ldots, a_n)$ mod q such that $a_1 + \cdots + a_n = 1$. Evaluate $J(\chi_1, \ldots, \chi_n)$ in terms of Gauss sums under suitable hypotheses on the χ_i. What is the analogous formula for definite integrals?

11. Let χ be the Legendre symbol modulo an odd prime q. Evaluate $\tau(\chi)^n$ in two ways to count the number of solutions mod q of $x_1^2 + \cdots + x_n^2 = 1$. If n is also an odd prime, use your formula to recover Quadratic Reciprocity (Hint: how many solutions are fixed under cyclic permutation of the x_i?). Can you modify this proof to also obtain the supplementary formula $(2/q) = \chi_8(q)$?

This proof of Quadratic Reciprocity can be modified to avoid explicit use of $\tau(\chi)$, because the solutions of $x_1^2 + \cdots + x_n^2 = 1$ can also be enumerated inductively by elementary means starting from results such as the parametrization of Pythagorean triples.

The usual way to recover Quadratic Reciprocity from the fact that $\tau(\chi)^2 = q^* = \pm q$ is to compare $\tau(\chi)$ with $\tau_n(\chi)$ mod n. On the one hand, they differ by a factor $\chi(n)$. On the other hand, if n is prime then $\tau_n(\chi) \equiv \tau(\chi)^n$ mod n, and thus equals $\tau(\chi)$ or $-\tau(\chi)$ according as q^* is a square mod n or not.

12. [Jacobi sums and Fermat curves mod q.] Let q be a prime, n a positive integer, and G the group of Dirichlet characters χ mod q such that $\chi^n = 1$. This is a cyclic group of order $\gcd(n, q-1)$ (why?). Prove that $\sum_{\chi,\chi' \in G} J(\chi, \chi')$ is the number of solutions of $x^n + y^n = 1$ in nonzero $x, y \in \mathbf{Z}/q\mathbf{Z}$. Conclude that this number is $q + O(n^2 q^{1/2})$, and thus that if "Fermat's Last Theorem" holds in $\mathbf{Z}/q\mathbf{Z}$ then $q \ll n^4$.

More precisely, the "Fermat curve" $F_n : x^n + y^n = z^n$ in the projective plane over $\mathbf{Z}/q\mathbf{Z}$ has $q + 1 - \sum_i \lambda_i$ points, where each λ_i is $-J(\chi, \chi')$ for one of the $(|G|-1)(|G|-2)$ choices of $\chi, \chi' \in G$ such that $\chi, \chi', \chi\chi'$ are all nontrivial. In particular, if $q \equiv 1$ mod n then $(|G|-1)(|G|-2) = (n-1)(n-2) = 2g$ where g is the genus of F_n. In this case the λ_i are the "eigenvalues of Frobenius" of F_n, and the fact that they all have norm $q^{1/2}$ is a special case of the Riemann hypothesis for the function field of an algebraic curve over a finite field. (If q is coprime to n but not 1 mod n then F_n still has $(n-1)(n-2)$ eigenvalues of Frobenius, which include the Jacobi sums but also other eigenvalues whose effect on the point counts of F_n appears only over finite extensions of $\mathbf{Z}/q\mathbf{Z}$.)

The last Exercise develops these ideas further for two curves of genus 1: the cubic Fermat curve F_3, and a quotient of F_4 whose $\mathbf{Q}$-rational points were determined by Fermat.

13. i) Suppose q is a prime congruent to 1 mod 3. It is known that q can be written uniquely as $(a^2 + 27b^2)/4$ for some positive integers a, b. Show that the number of solutions of $x^3 + y^3 = 1$ with $x, y \in \mathbf{Z}/q\mathbf{Z}$ is $q - 2 \pm a$, and determine the correct sign. Conclude that 2 is a cube mod q if and only if $2|a$, i.e., if and only if $q = m^2 + 27n^2$.
ii) Suppose q is an odd prime. How many solutions mod q do the equations $y^2 = x^4 - 1$ and $y^2 = x^3 - x$ have? (This should be easy if $q \equiv -1$ mod 4; for $q \equiv +1$ mod 4, cf. the previous $1\frac{1}{2}$ Exercises.)

These enumerations of rational points on $x^3 + y^3 = 1$ and $y^2 = x^3 - x$ mod q are now known to be special cases of the arithmetic of elliptic curves of complex multiplication; see for instance [Silverman 1986].

References

[Davenport 1967] Davenport, H.: *Multiplicative Number Theory.* Chicago: Markham, 1967; New York: Springer-Verlag, 1980 (GTM 74). [9.67.6 & 9.80.6 / QA 241.D32]

[Serre 1973] Serre, J.-P.: *A Course in Arithmetic.* New York: Springer, 1973 (GTM **7**). [AB 9.70.4 (reserve case) / QA243.S4713]

[Silverman 1986] Silverman, J.H.: *The Arithmetic of Elliptic Curves.* New York: Springer, 1986. [AB 9.86.1 (reserve case) / QA567.S44]