ZETA AND L-FUNCTIONS
OPEN DOOR SET

Problems:

(1) Write ξ and ψ 25 times each.

(2) In the proof of Dirichlet's theorem in class, it was asserted that

$$\zeta(0) = -\frac{1}{2}, \quad L(0,\chi) = -\frac{1}{m}\sum_{j=1}^{m} \chi(j)j$$

for χ a nontrivial Dirichlet character mod m. We never did fully explain why $\zeta(s)$ and $L(s,\chi)$ extend beyond the region $s > 0$. Here we sketch a nonrigorous argument (going back to Euler) for these computations at $s = 0$. The basic idea is that at $s = 0$, the Dirichlet series $\sum_{n\geq 1} a_n n^{-s}$ wants to be $\sum_{n\geq 1} a_n$, but this sum might not converge. How can we make sense of a nonconvergent sum, at least heuristically?

We define a sum $\sum_{n\geq 1} c_n$ to be *Abel summable* to α if $\sum_{n\geq 1} c_n x^n$ converges for $|x| < 1$ and tends to α as $x \to 1^-$.

a) Show $\sum_{n\geq 1}(-1)^{n-1}$ is Abel summable to 1/2. Using the Dirichlet series $\zeta_2(s) = (1 - 2^{1-s})\zeta(s)$, which converges for $s > 0$, give a heuristic argument that $\zeta(0)$ should be $-1/2$.

b) For $|r| < 1$, show $\sum_{n\geq 1} r^n$ is Abel summable to $r/(1-r)$.

c) If $\sum_{n\geq 1} c_n$ converges in the usual sense, say to S, show $\sum_{n\geq 1} c_n$ is Abel summable to S. Therefore the process of Abel summation does not change the value of a series which converges in the usual sense.

d) For a nontrivial Dirichlet character χ mod m, show $\sum_{n\geq 1} \chi(n)$ is Abel summable to $-(1/m)\sum_{j=1}^{m} \chi(j)j$, so this ought to be the value of $L(0,\chi)$.

e) For a squarefree integer $d \equiv 1 \bmod 4$, show $-(1/m)\sum_{j=1}^{m} (\frac{d}{j})j = 0$ if and only if $d > 0$.

Let $\chi_d(n) = (\frac{d}{n})$. If we accept that $L(s,\chi_d)$ can be extended beyond $s > 0$, and the finite sum in part d) is $L(0,\chi_d)$, then the fact (from the PROMYS number theory sets) that $x^2 - dy^2 = 1$ has a nontrivial integer solution for nonsquare $d > 0$ lets us interpret the equivalence of part e) as: $L(0,\chi_d) = 0$ if and only if $x^2 - dy^2 = 1$ has a nontrivial integer solution. So the vanishing of an L-function (at a point where it does not easily make any sense!) is equivalent to a certain Diophantine equation having a nontrivial solution.

(3) Taking for granted the Prime Number Theorem and Dirichlet's theorem in their natural density formulations, show

$$\#\{(\pi) : |N\pi| \leq x\} \sim \frac{x}{\log x},$$

where (π) runs over nonassociate irreducible elements in $\mathbf{Z}[i]$. Show the same result for $\mathbf{Z}[\sqrt{2}]$. Explain why the primes in $\mathbf{Z}[i]$ coming from integer primes which are $\equiv 3 \bmod 4$ have density 0 among the primes in $\mathbf{Z}[i]$, and therefore play no role in these asymptotics. Also determine an analogous set of negligible primes in $\mathbf{Z}[\sqrt{2}]$.

(4) Let $\chi\colon \mathbf{Z}[i] - \{0\} \to \mathbf{C}^\times$ by

$$\chi(\alpha) = \left(\frac{\alpha}{|\alpha|}\right)^4 = \frac{\alpha^4}{(N\alpha)^2}.$$

Note $|\chi(\alpha)| = 1$ and $\chi(\alpha)$ is unchanged if we multiply α by a unit.

Set $L(s,\chi) = \sum_{(\alpha)} \chi(\alpha) N\alpha^{-s}$ for $s > 1$. Express $L(s,\chi)$ as a quadratic Euler product over the primes in $\mathbf{Z}$ (that is, for all but finitely many p, the Euler factor at p will be a reciprocal quadratic polynomial in p^{-s}), and give a formula for the coefficients in these quadratic polynomials, in terms of arithmetic properties of p.

(5) (Another application of Dirichlet's theorem)

Fix a positive integer N. We define

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbf{Z}, ad - bc = 1, c \equiv 0 \bmod N \right\}.$$

This is the set of integer matrices with determinant 1, having the additional property that the lower left entry is divisible by N. Note $(d,N) = 1$ since $N|c$.

Another way to describe a typical element in $\Gamma_0(N)$ is as an integer matrix with determinant 1 which looks like $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$ modulo N.

a) Show $\Gamma_0(N)$ is a noncommutative group under matrix multiplication.

b) If d is an integer with $(d,N) = 1$, show there is a matrix in $\Gamma_0(N)$ with lower right entry d.

c) Let χ be a Dirichlet character mod N. Show $\psi\colon \Gamma_0(N) \to \mathbf{C}^\times$ by $\psi\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \chi(d)$ is multiplicative (i.e., $\psi(\gamma_1\gamma_2) = \psi(\gamma_1)\psi(\gamma_2)$ for γ_1, γ_2 in $\Gamma_0(N)$). Trivially $\psi\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) = 1$.

d) We now use Dirichlet's theorem to give a converse to part c). Let $\psi\colon \Gamma_0(N) \to \mathbf{C}^\times$ be multiplicative *and* assume that $\psi\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) = 1$.

Suppose that when $\left(\begin{smallmatrix} * & * \\ * & p \end{smallmatrix}\right)$ is in $\Gamma_0(N)$, for p an odd prime > 0, that $\psi\left(\begin{smallmatrix} * & * \\ * & p \end{smallmatrix}\right)$ depends only on $p \bmod N$ (not on the other matrix entries, nor on p for anything other than its mod N congruence class). Use Dirichlet's theorem to show that for any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\Gamma_0(N)$, $\psi(\gamma)$ only depends on $d \bmod N$, and the function $d \mapsto \psi(\left(\begin{smallmatrix} * & * \\ * & d \end{smallmatrix}\right))$ is a Dirichlet character mod N.

(Hint: $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$.)

Such functions ψ arise naturally as the "multiplier system for a weight 1 modular form on $\Gamma_0(N)$." An example of a weight 1 modular form on $\Gamma_0(3)$ is the doubly infinite series

$$\theta(z) = \sum_{m,n \in \mathbf{Z}} e^{2\pi i (m^2 - mn + n^2) z},$$

where z is in the upper half-plane. For any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\Gamma_0(3)$, it can be shown that

$$\theta(\gamma z) = \left(\frac{d}{3}\right)(cz+d)\theta(z),$$

where $\gamma z = (az+b)/(cz+d)$. (The matrices act on the upper half-plane by linear fractional transformations.) In this case, the function ψ is essentially the Legendre symbol $(\frac{\cdot}{3})$. Since $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)z = z+1$, the fact that $\psi\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) = 1$ in this case comes from $\theta(z)$ satisfying $\theta(z+1) = \theta(z)$.

(6) Recall in class that we introduced the polynomials $[M](X) \in \mathbf{F}_p[T][X]$ recursively, by: $[1](X) = X$, $[T](X) = X^p + TX$, $[T^j](X) = [T]([T^{j-1}](X))$ for $j \geq 2$, and

$$[c_n T^n + \cdots + c_1 T + c_0](X) = c_n [T^n](X) + \cdots + c_1 [T](X) + c_0 X.$$

a) Show $\deg[M](X) = p^{\deg M} = N(M)$ and $[M](X) = \sum_{j=0}^{\deg M} a_j(T) X^{p^j}$, where $a_0(T) = M$. (That is, $[M](X) \equiv MX \bmod X^2$.)

b) For M_1 and M_2 in $\mathbf{F}_p[T]$, show

$$[M_1 + M_2](X) = [M_1](X) + [M_2](X), \quad [M_1 M_2](X) = [M_1]([M_2](X)).$$

c) For $f \in \mathbf{F}_p[T][X]$ and monic irreducible $\pi \in \mathbf{F}_p[T]$, show $f([\pi](X)) = f(X)^{N\pi}$ in $(\mathbf{F}_p[T]/\pi)[X]$. This is an analogue of: $f(X^p) = f(X)^p$ in $(\mathbf{Z}/p)[X]$ for any f in $\mathbf{Z}[X]$.

d) Accept that there is a field $L \supset \mathbf{F}_p(T)$ in which $[M](X)$ splits into linear factors. Show all the roots of $[M](X)$ in L are distinct. (Hint: Consider the derivative of $[M](X)$ with respect to X, trying $M = T$ to get a sense of what's going on.)

e) Let Λ_M be all the roots of $[M](X)$ (in a field in which $[M](X)$ splits into linear factors). This additive group Λ_M is analogous to the multiplicative group of mth roots of unity in $\mathbf{C}$. For $A, B \in \mathbf{F}_p[T]$, prove

$$[A](\alpha) = [B](\alpha) \text{ for all } \alpha \in \Lambda_M \iff A \equiv B \bmod M.$$

This is the analogue of: $\omega^a = \omega^b$ for all mth roots of unity ω if and only if $a \equiv b \bmod m$.

f) For *monic* M, set

$$\Phi_M(X) = \prod_{\substack{[M](\omega)=0 \\ [D](\omega)\neq 0}} (X - \omega),$$

where the product is taken over roots of $[M](X)$ which are not roots of $[D](X)$ for any monic proper divisor D of M. This is an analogue of the mth cyclotomic polynomial. Show $[M](X) = \prod_{D|M} \Phi_D(X)$, the product taken over the monic divisors D of M, and $\Phi_M(X) \in \mathbf{F}_p[T][X]$. (A priori, the coefficients of $\Phi_M(X)$ as a polynomial in X are merely in some huge field containing $\mathbf{F}_p(T)$.)

g) Give an elementary proof that there are infinitely many monic irreducible π in $\mathbf{F}_p[T]$ such that $\pi \equiv 1 \bmod M$.

h) Show $\Phi_M(X)$ is irreducible in $\mathbf{F}_p(T)[X]$. (This is the analogue of $\Phi_m(X)$ being irreducible in $\mathbf{Q}[X]$. Take a proof you know or can read about in the cyclotomic polynomial case and make appropriate changes so the proof applies to $\Phi_M(X)$.)

i) (For those who know Galois theory) Let $F = \mathbf{F}_p(T)$. Prove $F(\Lambda_M)/F$ is a Galois extension with degree $\varphi(M)$, and there is a natural isomorphism from the Galois group of this field extension to $(\mathbf{F}_p[T]/M)^\times$. (Those who know algebraic number theory should also show that a monic irreducible of $\mathbf{F}_p[T]$ which does not divide M is unramified in this field extension and its corresponding Frobenius element in the Galois group is just the congruence class of the polynomial mod M.) The results of this part are completely analogous to what happens with cyclotomic extensions of $\mathbf{Q}$, so you should simply check that proofs in the cyclotomic case carry over to this new setting.

(7) (Reciprocity Law in Finite Fields) We saw in class that Kornblum's theorem can be applied to say something about quadratic residues in $\mathbf{F}_p[T]$ once we have a decent formulation of quadratic reciprocity in $\mathbf{F}_p[T]$. This was treated in class, and here we extend that reciprocity law to higher order residue symbols.

Fix a positive integer n and a prime $p \equiv 1 \bmod n$. Since $\mathbf{F}_p^\times$ is cyclic, there are n different nth roots of unity in $\mathbf{F}_p$.

a) Let $\mathbf{F}$ be a finite field containing $\mathbf{F}_p$, with $q = \#\mathbf{F}$. Show the nonzero nth powers in $\mathbf{F}$ are the solutions of $x^{(q-1)/n} = 1$.

b) Let π be irreducible in $\mathbf{F}_p[T]$. For f not divisible by π, define $(\frac{f}{\pi})_n$ to be the nth root of unity ω in $\mathbf{F}_p$ such that

$$f^{(N\pi-1)/n} \equiv \omega \bmod \pi.$$

Show there really is such an nth root of unity in $\mathbf{F}_p$, and that the nth power residue symbol is multiplicative: $(\frac{fg}{\pi})_n = (\frac{f}{\pi})_n(\frac{g}{\pi})_n$ for f and g not divisible by π.

c) For distinct monic irreducibles π_1 and π_2 in $\mathbf{F}_p[T]$, express $(\frac{\pi_2}{\pi_1})_n$ in terms of $(\frac{\pi_1}{\pi_2})_n$. (The case $n = 2$ and p odd is quadratic reciprocity.)

(8) Let $\mathbf{F}$ be any finite field, not necessarily a field of prime size.

a) Define $\zeta_{\mathbf{F}[Y]}(s)$ and $L(s, \chi)$, where χ is a character of some group $(\mathbf{F}[Y]/M(Y))^\times$.

b) Extend these zeta and L-functions to all s (except at $s = 1$ for the zeta function).

c) Let $\mathbf{F}$ contain $\mathbf{F}_p$, and $\#\mathbf{F} = p^d$. Define $\mathrm{Tr}\colon \mathbf{F} \to \mathbf{F}_p$ by

$$\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{d-1}}.$$

This is an additive function, called the trace from $\mathbf{F}$ to $\mathbf{F}_p$. Check its values are in $\mathbf{F}_p$, and it does not always take the value 0.

d) Suppose p is odd, and let π be monic irreducible in $\mathbf{F}_p[T]$ of degree d. Find a Dirichlet character on $(\mathbf{F}_p[T]/\pi)[Y]$ with L-function $1 + a_1 p^{-ds}$, where

$$a_1 = \sum_{f \in \mathbf{F}_p[T]/\pi} \left(\frac{f}{\pi}\right) \omega^{\mathrm{Tr}(f \bmod \pi)}.$$

Here ω is a nontrivial pth root of unity in $\mathbf{C}$ (so raising it to a power in $\mathbf{F}_p = \mathbf{Z}/p$ makes sense) and Tr is the trace function from $\mathbf{F}_p[T]/\pi$ to $\mathbf{F}_p$.

This sum a_1 is a more general type of Gauss sum than what we met on Set 5; that its absolute value is $\sqrt{p^d}$ can be proved by elementary methods or as a consequence of an appropriate Riemann Hypothesis.

(9) For real numbers a and b, write

$$\frac{1}{1-ax+bx^2} = \sum_{n\geq 0} c_n x^n, \qquad 1-ax+bx^2 = (1-\alpha x)(1-\beta x).$$

Show the following statements are equivalent:

i) $|\alpha| = |\beta| = 1/\sqrt{b}$.

ii) $|a| \leq 2\sqrt{b}$.

iii) For all $\varepsilon > 0$, $|c_n/b^{n(1/2+\varepsilon)}|$ is bounded independently of n (but possibly depending on ε).

This exercise equates a Riemann hypothesis with an upper bound on one number and a growth estimate on a sequence of numbers.

(10) Let d be a squarefree integer (e.g., 2, -3, or 10). Set

$$N_{p,d} = \#\{(x,y) \in \mathbf{Z}/p \times \mathbf{Z}/p : y^2 = x^3 - d^2x\}.$$

The numbers $N_{p,1}$ were met on Set 5, where they were written as N_p.

Set $a_{p,d} = p - N_{p,d}$, so (by Set 5, exer. 2) $a_{p,1} = a_p$ is the pth Dirichlet coefficient of the Hecke L-function from Set 4, exercise 7. Show the L-function

$$L_d(s) = \prod_{(p,2d)=1} \frac{1}{1 - a_{p,d}p^{-s} + p \cdot p^{-2s}}$$

converges for $s > 3/2$ and its Dirichlet series is a twist by the quadratic character $(\frac{d}{\cdot})$ of the ordinary Dirichlet series for the Hecke L-function from Set 4. Here we use the word "twist" in the sense of Set 3, exercise 4.

(It can be shown that $L_d(s)$ extends naturally to all s. A difficult theorem of Coates and Wiles says that if the equation $y^2 = x^3 - d^2x$ has a nontrivial rational solution – i.e., a rational solution other than $(0,0)$, $(d,0)$, and $(-d,0)$ – then $L_d(1) = 0$. A conjecture of Birch and Swinnerton–Dyer says the converse is also true: if $L_d(1) = 0$, then the equation $y^2 = x^3 - d^2x$ admits a nontrivial rational solution. This converse direction can be proved in a large number of cases by work of Gross and Zagier.

This connection between vanishing of an L-function and existence of a nontrivial solution to a Diophantine equation is analogous to the Diophantine interpretation of part e) of the second exercise on this Open Door set.)