ZETA AND L-FUNCTIONS
HOMEWORK 3
JULY 13, 2000

Due: Thursday, July 20 at the beginning of class

Problems:

(1) Verify the following identities, for $s > 1$:

$$\sum_{n\geq 1} \frac{|\mu(n)|}{n^s} = \frac{\zeta(s)}{\zeta(2s)}, \qquad \sum_{n\geq 1} \frac{\tau(n)^2}{n^s} = \frac{\zeta(s)^4}{\zeta(2s)}.$$

(2) Define

$$\zeta_2(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots = \sum_{n\geq 1} \frac{(-1)^{n-1}}{n^s}.$$

a) Show $\zeta_2(s)$ converges for $s > 0$, and when $s > 1$ we have

$$\zeta_2(s) = (1 - 2^{1-s})\zeta(s).$$

Therefore the formula $\zeta_2(s)/(1-2^{1-s})$ provides us with a means of extending the definition of $\zeta(s)$ to $s > 0$ (with $\zeta(1) = \infty$).

b) For any integer $m \geq 2$, let

$$\begin{aligned} \zeta_m(s) &= 1 + \frac{1}{2^s} + \cdots + \frac{1}{(m-1)^s} - \frac{m-1}{m^s} + \dots \\ &= \sum_{n\geq 1} \frac{a_n}{n^s}, \end{aligned}$$

where $a_n = 1$ for $n \not\equiv 0 \bmod m$ and $a_n = -(m-1)$ for $n \equiv 0 \bmod m$. Show $\zeta_m(s)$ converges for $s > 0$ and $\zeta_m(s) = (1 - m^{1-s})\zeta(s)$ when $s > 1$. Therefore we can extend $\zeta(s)$ from $s > 1$ to $s > 0$ by the formula

$$\frac{\zeta_m(s)}{1 - m^{1-s}}.$$

Show this ratio of functions does not depend on the choice of $m \geq 2$, so we do not get different extensions of the zeta function by using different values of m. (Note: Be careful about how you work with the series $\zeta_m(s)$ for $0 < s < 1$, where the series can't be arbitrarily rearranged.)

c) With the extension of $\zeta(s)$ to $0 < s < 1$ as given in part a), show $\zeta(s) < 0$ for $0 < s < 1$.

(3) Determine all Dirichlet characters mod 9 and mod 12. (For modulus 9, you will need cube roots of unity. Write ω for $(-1 + \sqrt{3}i)/2$, a nontrivial cube root of unity.)

(4) Let $f(s) = \sum_{n\geq 1} a_n n^{-s}$ be a Dirichlet series and χ be a Dirichlet character. For a Dirichlet character χ, define the *twist* of f by χ to be the Dirichlet series $f_\chi(s) = \sum_{n\geq 1} a_n \chi(n) n^{-s}$. For example, the twist of $\zeta(s)$ by χ_3 is $L(s, \chi_3)$.

For Dirichlet series f and g which converge somewhere and χ a Dirichlet character, show $(f+g)_\chi(s) = f_\chi(s) + g_\chi(s)$ and $(fg)_\chi(s) = f_\chi(s) g_\chi(s)$, where the equations hold for large s. (How large does s have to be?) So twisting a Dirichlet series by a Dirichlet character commutes with addition and multiplication of the series.

(5) Suppose $\sum a_n n^{-s}$ is a Dirichlet series admitting a quadratic Euler product:

$$\sum_{n\geq 1} \frac{a_n}{n^s} = \prod_p \frac{1}{1 - a_p p^{-s} + b_p p^{-2s}}.$$

a) Notice that a_p appears in two places, as the coefficient of the pth term in the sum on the left and as a coefficient in the pth factor on the right. Show this is not inconsistent, in the sense that if we assumed instead the a priori more general quadratic Euler product

$$\sum_{n\geq 1} \frac{a_n}{n^s} = \prod_p \frac{1}{1 - c_p p^{-s} + b_p p^{-2s}},$$

then $c_p = a_p$.

b) Show $a_{p^r} = a_p a_{p^{r-1}} - b_p a_{p^{r-2}}$ for $r \geq 2$. (In particular, if $b_p = 0$, so the pth Euler factor has degree less than 2, then we get $a_{p^r} = a_p^r$.)

c) When $a_n = \sigma_k(n)$, find b_p.

(6) For $\alpha = a + b\sqrt{2}$ in $\mathbf{Z}[\sqrt{2}]$, its norm is $N\alpha = a^2 - 2b^2$ and this norm is multiplicative by simple algebraic calculations. Since $N(2 + 3\sqrt{2}) = -14$, the norm can be negative.

a) For nonzero α in $\mathbf{Z}[\sqrt{2}]$, prove $\#\mathbf{Z}[\sqrt{2}]/\alpha = |N\alpha|$. (In this and the rest of this problem, which is a generalization of an earlier exercise for $\mathbf{Z}[i]$, don't just say "This is the same as $\mathbf{Z}[i]$." Work out the details, in your own words.)

b) Define the zeta function of $\mathbf{Z}[\sqrt{2}]$ to be

$$\zeta_{\mathbf{Z}[\sqrt{2}]}(s) = \prod_{(\pi)} \frac{1}{1 - |N\pi|^{-s}},$$

where $\prod_{(\pi)}$ designates a product over nonassociate irreducibles of $\mathbf{Z}[\sqrt{2}]$. (Associate elements have the same norm, and there are infinitely many units, so it is pretty important here that we *not* be taking a product over *all* the irreducibles!)

Prove the Euler product defining $\zeta_{\mathbf{Z}[\sqrt{2}]}(s)$ converges for $s > 1$ and then show

$$\zeta_{\mathbf{Z}[\sqrt{2}]}(s) = \sum_{(\alpha)} \frac{1}{|N\alpha|^s},$$

where $\sum_{(\alpha)}$ is a summation over nonassociate elements of $\mathbf{Z}[\sqrt{2}]$. Explicitly cite any convergence theorems you use for infinite series and products, as well as any arithmetic properties you use of $\mathbf{Z}[\sqrt{2}]$.

c) For $s > 1$, prove $\zeta_{\mathbf{Z}[\sqrt{2}]}(s) = \zeta(s)L(s, \chi_8^+)$, where χ_8^+ is the mod 8 Dirichlet character that equals 1 on ± 1.

d) For $s > 1$, show $\zeta_{\mathbf{Z}[\sqrt{2}]}(s) \leq \zeta(s)^2$. The same argument should show $\zeta_{\mathbf{Z}[i]}(s) \leq \zeta(s)^2$.

(7) This exercise gives a purely algebraic proof that for $n \geq 2$, there are infinitely many primes $p \equiv 1 \bmod m$. It generalizes the proof from class that there are infinitely many $p \equiv 1 \bmod 4$.

Although it may seem pedantic, you are reminded that primes are understood to be positive.

We will use the mth *cyclotomic polynomial* $\Phi_m(X)$, which is defined to be the polynomial whose roots are the different roots of unity of exact order m:

$$\Phi_m(X) = \prod (X - \omega),$$

where ω runs over the mth roots of unity in $\mathbf{C}$ with exact order m. For example,

$$\Phi_1(X) = X - 1, \quad \Phi_2(X) = X + 1, \quad \Phi_3(X) = X^2 - X + 1, \quad \Phi_4(X) = X^2 + 1.$$

Collecting the mth roots of unity according to their exact order, we have the basic identity

$$X^m - 1 = \prod_{d|m} \Phi_d(X).$$

The salient nontrivial fact you need to know about cyclotomic polynomials is that $\Phi_m(X) \in \mathbf{Z}[X]$ for all m. (From their definition, it is only apparent that $\Phi_m(X) \in \mathbf{C}[X]$.) In particular, the above equation now implies $\Phi_m(X) | (X^m - 1)$ in $\mathbf{Z}[X]$ for all m.

a) Prove $\Phi_m(0) = 1$ for $m \geq 2$.

b) By definition, $\Phi_m(X)$ is constructed so that its roots in $\mathbf{C}$ are the roots of unity of exact order m, each root appearing once. Since $\Phi_m(X)$ has coefficients in $\mathbf{Z}$, the polynomial can be reduced mod p and we may consider roots in $\mathbf{Z}/p$ of the mod p mth cyclotomic polynomial. Prove that when p does not divide m, the roots of $\Phi_m(X)$ in $\mathbf{Z}/p$ – if there are any – have the same algebraic property as the complex roots: they appear only once and have (multiplicative) order m. That is, if $\Phi_m(r) \equiv 0 \bmod p$ with p not dividing m, then $(X - r)^2$ is not a factor of $\Phi_m(X)$ in $(\mathbf{Z}/p)[X]$ and r has order m in $(\mathbf{Z}/p)^\times$.

In particular, if p does not divide m and $\Phi_m(r) \equiv 0 \bmod p$ for some integer r, then PROMYS number theory implies $m | p - 1$, so $p \equiv 1 \bmod m$. (If we did not take primes to be positive, we'd have to write this conclusion as $|p| \equiv 1 \bmod m$, since $\#(\mathbf{Z}/p) = |p|$ if we make no convention on the sign of prime numbers.)

c) Fix $m \geq 2$. Show $\Phi_m(a) \neq \pm 1$ for large a. By choosing a appropriately, deduce that there is a (positive) prime $p \equiv 1 \bmod m$, and then construct infinitely many such primes.

d) For $m \geq 3$, prove there are infinitely many (positive) primes $p \not\equiv 0, 1 \bmod m$. (At some point in the proof you'd better use the fact that $m \neq 2$, since the result is false when $m = 2$. Point out where $m \neq 2$ is used.)

e) The salient nontrivial fact referred to above, that $\Phi_m(X)$ has integer coefficients, can be proven without much trouble via infinite series, as follows.

We take $m \geq 2$; the result is clear for $m = 1$. Argue by a multiplicative Möbius inversion that

$$\Phi_m(X) = \prod_{d|m} (X^d - 1)^{\mu(m/d)} = \prod_{d|m} (1 - X^d)^{\mu(m/d)},$$

where the order of subtraction can be switched since $\sum_{d|m} \mu(m/d) = 0$ for $m \geq 2$. Convert any terms $(1 - X^d)^{-1}$ having an exponent of -1 into a geometric series, multiply all factors of the product together, and then compare with the original definition of $\Phi_m(X)$.

f) Just to be clear about what is going on with "additive" and "multiplicative" Möbius inversions, let's prove a generalized Möbius inversion formula. Let A be any abelian group, with the group operation written additively. Let f, g be two functions from $\mathbf{Z}^+$ to A having the relation $f(n) = \sum_{d|n} g(d)$ for all n. Observe the addition here is taking place in the group A. Prove $g(n) = \sum_{d|n} \mu(n/d) f(d)$. Part e) is Möbius inversion where $f(n) = X^n - 1$ and $g(n) = \Phi_n(X)$ send $\mathbf{Z}^+$ to the *multiplicative* group of rational functions.