MATH 7230 Homework 8 - Spring 2017

Due Thursday, Apr. 12 at 10:30

You are required to turn in at least **one** of the following problems, and must complete a total of **20** by semester's end. Group work is allowed, but your solutions must be written up individually.

The notation "MV A.B.C" means Exercise C at the end of Section A.B in the textbook (Montgomery-Vaughan).

Problems 1–3 address some properties of cyclotomic polynomials, which primarily arise in the study of characters for the **additive** groups of integers modulo m (in contrast to Dirichlet characters, which are for the *multiplicative* groups). In these problems you will prove much of the content of MV 4.1.9 (although with somewhat shorter/simpler arguments than those outlined in the textbook).

1. For a positive integer q, the *cyclotomic polynomial* is defined by

$$\Phi_q(z) := \prod_{\substack{1\le n\le q\\ (n,q)=1}} \left(z - \zeta_q^n\right), \tag{1}$$

where $\zeta_n := e^{\frac{2\pi i}{n}}$ is the (canonical) primitive n-th root of unity.

(a) The Fundamental Theorem of Algebra implies that

$$z^q - 1 = \prod_{1\le n\le q} \left(z - \zeta_q^n\right).$$

Use this to prove that

$$z^q - 1 = \prod_{d|q} \Phi_d(z). \tag{2}$$

Remark: The cyclotomic polynomials are sometimes alternatively defined using (2)*, which gives the recursive formula*

$$\Phi_q(z) := \frac{z^q-1}{\prod\limits_{d|q,\ d<q} \Phi_d(z)}.$$

The advantages of this definition are that it allows one to compute $\Phi_q(z)$ without using any complex coefficients. In fact, this shows that $\Phi_q(z)$ is a series with integer coefficients; however, it is not immediately clear that they are actually polynomials.

(b) Denote $f_m(z) := z^m - 1$. Prove that

$$\Phi_q(z) = \prod_{d|q} f_d(z)^{\mu\left(\frac{q}{d}\right)}. \tag{3}$$

Hint: The most compact proof follows from taking the logarithm of (2) *and applying Möbius inversion. Alternatively, one can carefully calculate the total exponent of each factor $(z - \zeta_q^n)$ on the right side of* (2)*, using* (1)*.*

(c) Conclude that $\Phi_q(z) \in \mathbb{Z}[z]$.

2. (a) Give a formula for $\Phi_q(z)$ if $q = p^k$, where p is prime.

   (b) Prove that
$$\Phi_q(1) = \begin{cases} p & \text{if } q = p^k, \\ 1 & \text{otherwise.} \end{cases}$$
   Hint: One approach is to use (3) *to show that* $\Phi_q(1) = \prod_{d \mid q} d^{\mu\left(\frac{q}{d}\right)}$. *Then take the logarithm and use properties of the von Mangoldt function* $\Lambda(n)$.

3. In Homework 1 Problem 3 you used simple properties of subgroups in $(\mathbb{Z}/q\mathbb{Z})^\times$ to prove that there are infinitely many primes $p \not\equiv 1 \pmod{q}$. In this problem you will use cyclotomic polynomials to prove the complementary fact (and special case of Dirichlet's theorem) that there are infinitely many primes $p \equiv 1 \pmod{q}$.

   (a) Prove that $\Phi_q(n) \to \infty$ as $n \to \infty$.
   Hint: It is sufficient to show that $\Phi_q(z)$ *is a monic polynomial.*

   (b) Suppose that p is prime and $p \nmid q$. Prove that if $\Phi_q(n) \equiv 0 \pmod{p}$, then $\text{ord}_p(n) = q$ (i.e., $n^r \not\equiv 1 \pmod{p}$ for any proper divisor $r \mid q, r \neq q$).
   Hint: Suppose to the contrary that $n^r - 1 \equiv 0 \pmod{p}$ *for some* $r \mid q$ *with* $r < q$. *Use* (2) *to conclude that* n *is a double root of* $z^q - 1 \bmod p$. *But then* $\frac{d}{dz}(z^q - 1) = qz^{q-1}$ *evaluated at* $z = n$ *is a multiple of* p *– why is this a contradiction?*

   (c) Now you will prove that there are infinitely many primes $p \equiv 1 \pmod{q}$. In particular, suppose that $p_1, \cdots, p_N$ are primes congruent to 1 mod q, and use part (a) to choose k such that $M := \Phi_q(kqp_1 \cdots p_N) > 1$. Now consider a prime divisor $p \mid M$, and show that $p \nmid qp_1 \cdots p_N$.

   (d) Finally, use part (b) to conclude that $q \mid (p-1)$, so that $p \equiv 1 \pmod{q}$. Use part (c) to conclude that $p \neq p_j$ for $1 \leq j \leq N$.

4. Both of these problems from the textbook are quite short! For both parts, start by expanding the sums using the fact that the complex modulus satisfies $|z|^2 = z \cdot \overline{z}$, and then use the orthogonality relations.

   (a) MV 4.2.2.

   (b) MV 4.2.3.

5. MV 4.2.4. For part (c), consider the sum
$$S(a, q) := \sum_{\chi \bmod q} \sum_{j=0}^{k-1} \left(\frac{\chi(a)}{\zeta} \right)^j,$$
and evaluate it in two different ways. First, use part (b) to simplify it as written, and second, interchange the summations and use orthogonality. Comparing the two resulting expressions gives the claim.

Remark: This problem immediately leads to an "algebraic" proof that
$$\zeta_m(s) := \prod_{\chi \bmod m} L(s, \chi) = \prod_{p \nmid m} \left(1 - \frac{1}{p^{\text{ord}_m(p)s}} \right)^{-\frac{\varphi(m)}{\text{ord}_m(p)}},$$

where $\mathrm{ord}_m(p)$ *denotes the order of* p *in the multiplicative group modulo* m*.*

Problems 6–7 address the functions used in Golomb's "Lambda method", which constructs a generalization of the von Mangoldt function to detect integers with a bounded number of distinct prime factors. Recall that von Mangoldt's function satisfies $\Lambda = \mu * \log$, so that

$$\Lambda(n) = \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right) = \begin{cases} \log p & \text{if } n = p^a; \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

Thus Λ is a (weighted) indicator function for integers that have at most 1 prime factor.

The generalized function is defined by

$$\Lambda_k(n) := \sum_{d|n} \mu(d) \left(\log\left(\frac{n}{d}\right)\right)^k .$$

6. (a) Prove (by direct computation) that $\Lambda(n) = 0$ if n has at least two distinct prime divisors. In other words, suppose that $n = p^a m$ where $a > 0, m > 1$ and $p \nmid m$, and plug in to the sum in (4).

   (b) Prove (by direct computation) that

$$\Lambda_2(n) = \begin{cases} 2\log p \log q & \text{if } n = p^a q^b, \text{ where } p, q \text{ are distinct primes;} \\ (2a-1)(\log p)^2 & \text{if } n = p^a. \end{cases}$$

   Remark: It is also true that $\Lambda_2(n) = 0$ *if* n *has at least three distinct prime divisors, but this is already a very involved calculation. The next problem provides a much more powerful way of understanding the* Λ_k*.*

7. Recall the typical notation for Dirichlet series: for a sequence or function $\{f(n)\}_{n=1}^{\infty}$, the corresponding Dirichlet series is

$$\alpha_f(s) := \sum_{n\geq 1} \frac{f(n)}{n^s}.$$

   (a) Recall that (or prove if you've never done so before)

$$\frac{d}{ds}\alpha_f(s) = -\alpha_{f\cdot\log}(s).$$

   Note that this is the product of f and log, **not** the convolution. Now use this to show that

$$\alpha_{\Lambda_k}(s) = (-1)^k \frac{\zeta^{(k)}(s)}{\zeta(s)}. \tag{5}$$

   (b) Using part (a) (specifically, take the derivative of (5)), prove the inductive formula

$$\alpha_{\Lambda_{k+1}}(s) = \alpha_{\Lambda_k\cdot\log}(s) + \alpha_{\Lambda_k}(s)\alpha_{\Lambda}(s).$$

   For example, this implies that $\Lambda_2 = \Lambda \cdot \log + \Lambda * \Lambda$, i.e.

$$\Lambda_2(n) = \Lambda(n)\log n + \sum_{d|n} \Lambda(d)\Lambda\left(\frac{n}{d}\right).$$

(c) Conclude inductively that $\Lambda_k(n) = 0$ if n has more than k distinct prime factors.

(d) Finally, prove that if $n = p_1^{a_1} \cdots p_k^{a_k}$, with p_j distinct and $a_j \geq 1$, then

$$\Lambda_k(n) = k! \log p_1 \cdots \log p_k.$$

In Problems 8– you will explore some properties of arithmetic density. If $A \subset B \subset \mathbb{N}$, then the *arithmetic (or natural) density* of A in B is

$$d_B(A) := \lim_{X\to\infty} \frac{\#\{n \leq X \mid n \in A\}}{\#\{n \leq X \mid n \in B\}}.$$

Similarly, assuming that B is *substantial* (so that $\sum_{n\in B} \frac{1}{n} = \infty$), the *logarithmic (Dirichlet) density* is

$$D_B(A) := \lim_{s\to 1^+} \frac{\displaystyle\sum_{n\in A} \frac{1}{n^s}}{\displaystyle\sum_{n\in B} \frac{1}{n^s}}.$$

8. (a) Let A be the set of positive integers whose first digit is 1. Prove that the arithmetic density of A does not exist.

   (b) Prove that the logarithmic density of A is $\log_{10} 2 \cong 0.301$.

   (c) Now let A' be the set of positive integers with **no** digits equal to 1. Prove that $d(A') = 0$. What is $D(A')$?

9. In this problem you will prove some general properties of densities. If the type of density is not specified, then the statement applies to both.

   (a) Prove that if A is finite, then the density of A is zero (relative to any infinite set).

   (b) Prove that if A_1, A_2 are disjoint and have densities δ_1, δ_2, respectively, then $A_1 \cup A_2$ has density $\delta_1 + \delta_2$.

   (c) Use (a) and (b) to conclude that if $\delta_1 + \delta_2 > 1$, then $A_1 \cap A_2$ is infinite.

   (d) Prove that if $d_B(A) = \delta$, then the logarithmic density is also $D_B(A) = \delta$.
   Hint: Use partial summation.