MATH 7230 Homework 3 - Spring 2014

Due Thursday, Mar. 6 at 1:30

The notation "I-K" is shorthand for the textbook.

1. In this problem you will prove that if q is prime, then there are infinitely many primes congruent to 1 mod q, filling in the details from I-K Section 2.3.

   (a) For prime q, the q-th *cyclotomic* polynomial is

   $$\Phi_q(x) = \frac{x^q - 1}{x - 1} = x^{q-1} + x^{q-2} + \cdots + x + 1.$$

   Show that if $p \mid \Phi_q(n)$, then $n^q \equiv 1 \pmod{p}$. Recall Fermat's Little Theorem (a special case of Lagrange's Theorem for finite groups), which states that $n^{p-1} \equiv 1 \pmod{p}$ if $p \nmid n$. Conclude that $q \mid (p-1)$.

   (b) Suppose that $p_1, \ldots, p_k$ are all primes congruent to 1 mod q. Let $n_k := p_1 \cdots p_k$ and apply part (a) to conclude that there is a new prime divisor $p \mid \Phi_q(n_k)$ such that $p \equiv 1 \pmod{q}$.

   (Optional) Using more general properties of cyclotomic polynomials, this proof can be extended to an arbitrary modulus q. For example, see: `http://ocw.mit.edu/courses/mathematics/18-781-theory-of-numbers-spring-2012/lecture-notes/MIT18_781S12_lec12.pdf`

2. Show that the characters on $G = \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ are given explicitly as χ_{a_1,a_2} for all pairs $a_i \in \mathbb{Z}/m_i\mathbb{Z}$, where

   $$\chi_{a_1,a_2}(n_1, n_2) = e\left(\frac{a_1 n_1}{m_1} + \frac{a_2 n_2}{m_2}\right).$$

3. Read the top half of page 44 in I-K. This problem provides a more general framework for characters that are trivial on a subgroup.

   Let G be a finite abelian group, and suppose that $H < G$ is a subgroup. Write

   $$\widehat{G}_H := \left\{\chi \in \widehat{G} \mid \chi(H) = 1\right\}.$$

   In other words, these are the characters that restrict to the trivial character χ_0 on H.

   (a) Prove that $\widehat{G}_H$ is a subgroup of $\widehat{G}$. What are $\widehat{G}_{\{1\}}$ and $\widehat{G}_G$?

   (b) Prove that $\widehat{G}_H \cong \widehat{G/H}$.

   (c) Similarly, prove that $\widehat{G}/\widehat{G}_H \cong \widehat{H}$.

   (d) Prove the orthogonality relation

   $$\sum_{\chi \in \widehat{G}_H} \chi(g) = \begin{cases} \frac{|G|}{|H|} & \text{if } g \in H, \\ 0 & \text{it } g \notin H. \end{cases}$$

(e) Part (d) implies that the indicator function for H can be written as

$$\mathbb{1}_H(g) = \frac{|H|}{|G|} \sum_{\chi \in \widehat{G}_H} \chi(g).$$

Use the standard orthogonality relations on G to prove the alternative expression

$$\mathbb{1}_H(g) = \sum_{h \in H} \delta_h(g) = \sum_{h \in H} \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi\left(h^{-1}g\right).$$

Can you show that expressions are equivalent?

(Optional) If G is nonabelian, is it necessarily true that $G \cong \widehat{G}$?
Hint: Consider a simple group, such as $G = A_n$.

4. If $\boldsymbol{a} = \{a_n\}_{n=1}^{\infty}$ is a sequence of complex numbers, define the Dirichlet series

$$L(s, \boldsymbol{a}) := \sum_{n \geq 1} \frac{a_n}{n^s}.$$

(a) Prove that if $\boldsymbol{a}$ is bounded, then $L(s, \boldsymbol{a})$ converges for $\mathrm{Re}(s) > 1$.

(b) Prove that if the partial sums $\sum_{n=1}^{k} a_n$ are bounded, then $L(s, \boldsymbol{a})$ converges for $\mathrm{Re}(s) > 0$.
Hint: Use partial summation.

5. Recall that in the proof of Dirichlet's Theorem we proved the following identity for the product of all L-functions for characters of $G := (\mathbb{Z}/q\mathbb{Z})^{\times}$:

$$\zeta_q(s) := \prod_{\chi \bmod q} L(s, \chi) = \prod_{p \nmid q} \left(\frac{1}{1 - p^{-o(p)s}} \right)^{\frac{\phi(q)}{o(p)}},$$

where $o(p) = \mathrm{ord}_q(p)$ is the order of p in G. We then concluded that $L(1, \chi) \neq 0$ for all $\chi \neq \chi_0$ by using a meromorphic continuation of $\zeta_q(s)$ to the half-plane $\mathrm{Re}(s) > 0$.

In this problem you will derive a proof of the non-vanishing of these L-values that does not require as much (or any) machinery from complex analysis.

(a) Prove that $\zeta_q(1) \neq 0$. Conclude that there is at most one χ such that $L(1, \chi) = 0$.

(b) A Dirichlet character $\chi \in \widehat{G}$ is a *real* character if $\chi(G) \subset \mathbb{R}$. A character that is not real is *complex.* Prove that if χ is a complex character, then $L(1, \chi) = 0$ if and only if $L(1, \overline{\chi}) = 0$. Conclude that none of these L-values are zero.

(c) Prove that χ is real if and only if $\chi^2 = \chi_0$. Equivalently, $\chi(g^2) = 1$ for any $g \in G$.

(d) It remains to show that $L(1, \chi) \neq 0$ for real $\chi \neq \chi_0$. Define

$$T(x) := \sum_{n \leq x} \frac{\tau(n, \chi)}{\sqrt{n}},$$

where $\tau(\bullet, \chi) := \mathbb{1} \star \chi$.

i. Prove that $\tau(n,\chi) \geq 0$ for all n and $\tau(m^2,\chi) \geq 1$.
Hint: Use multiplicativity.

ii. Conclude that $T(x) \geq \frac{1}{2}\log x$.

iii. Use the Hyperbola Method to prove $T(x) = \frac{1}{2}L(1,\chi)\sqrt{x} + O(1)$.
Hint: Write

$$\begin{aligned} T(x) &= \sum_{mn \leq x} \frac{\chi(m)}{\sqrt{mn}} \\ &= \sum_{m \leq \sqrt{x}} \frac{\chi(m)}{\sqrt{m}} \sum_{n \leq \frac{x}{m}} \frac{1}{\sqrt{n}} + \sum_{n < \sqrt{x}} \frac{1}{\sqrt{n}} \sum_{\sqrt{x} < m \leq \frac{x}{n}} \frac{\chi(m)}{\sqrt{m}}. \end{aligned}$$

The first sum will be the main term; use partial summation to bound the final sum on m.

iv. Take the limit as $x \to \infty$ and conclude that $L(1,\chi) > 0$.

(Optional) Read pages 36 – 37 of I-K to learn a proof of Dirichlet's Theorem that is more in the spirit of the elementary proof of the Prime Number Theorem.