18.781 ANALYTIC NUMBER THEORY QUIZ

Friday, Nov. 30, 2007

Name: ______________________________

Numeric Student ID: ____________________

Instructor's Name: ______________________

I agree to abide by the terms of the honor code:

Signature: ____________________________

Instructions: Print your name, student ID number and instructor's name in the space provided. During the test you may not use notes, books or calculators. Read each question carefully and **show all your work**; full credit cannot be obtained without sufficient justification for your answer unless explicitly stated otherwise. Underline your final answer to each question. There are 4 questions. You have 50 minutes to do all the problems.

Question	Score	Maximum
1		6
2		6
3		6
4(BONUS)		3
Total		18

1. Give an explicit definition of the characters $\chi_q : (\mathbb{Z}/q\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$, where q is prime. That is, provide a careful definition of such a function χ_q and then prove that your definition satisfies the necessary property of a character.

   Solution:

   Everything on this quiz can be found someplace in the notes posted online, so I will be relatively brief on these solutions.

   The character χ_q to the modulus q is defined by

   $$\chi_q(n) = \zeta_{q-1}^{\nu(n)}$$

   where ζ_{q-1} is a $(q-1)$st root of unity, and $\nu(n)$ is defined by the equation

   $$g^{\nu(n)} \equiv n\ (q), \quad g\text{: a primitive root mod } q.$$

   Since g is a primitive root, it's powers g^k give a complete reduced residue system mod q, and hence we may find such an exponent $\nu(n)$ satisfying the above congruence for any n with $q \nmid n$. Moreover, any other exponent $\nu'(n)$ satisfying this property differs from $\nu(n)$ by a multiple of $q-1$ (the order of g). This shows that χ_q does not depend on the choice $\nu(n)$ or $\nu'(n)$, since $\zeta_{q-1}^{\nu(n)} = \zeta_{q-1}^{\nu'(n)}$. (That's actually quite important, as our definition would not make sense without this fact.)

   To check that χ_q is a character, we must verify the multiplicative property $\chi_q(mn) = \chi_q(m)\chi_q(n)$. This follows easily from the above definitions together with the fact that

   $$\nu(mn) \equiv \nu(m) + \nu(n)\ (q-1)$$

2. Provide a definition for the Dirichlet series $L(s,\chi)$, for χ a character mod q, and then prove the following equality (for any non-zero residue a mod q):

$$\frac{1}{q-1}\sum_{\chi \bmod q} \bar{\chi}(a)\log(L(s,\chi)) = \sum_{p\colon \text{prime}} \sum_{\substack{m=1 \\ p^m \equiv a\ (q)}}^{\infty} \frac{1}{m} p^{-ms}$$

Solution:

This identity really comes straight from the notes, and is the key identity to setting up Dirichlet's theorem on primes. There are three main ingredient to proving it.

- $$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \neq q} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

  which is just like the Euler product for the Riemann zeta function. It still holds in this case because χ is a multiplicative function.

- Apply log to the above identity, and use the fact that, as a power series,

  $$-\log(1-x) = \sum_{m=1}^{\infty} \frac{x^m}{m}$$

- Finally, use the following all-important fact about characters:

  $$\sum_{\chi} \chi(n) = \begin{cases} q-1 & n \equiv 1\ (q) \\ 0 & \text{otherwise.} \end{cases}$$

  which is an easy consequence of our definition in the previous problem in terms of roots of unity, remembering that there are $q-1$ characters mod q which result from the distinct choices of roots of unity. From this, it follows that

  $$\sum_{\chi} \bar{\chi}(a)\chi(n) = \begin{cases} q-1 & n \equiv a\ (q) \\ 0 & \text{otherwise.} \end{cases}$$

  which gives the above equality.

3. Prove that the following statement is equivalent to Dirichlet's theorem on primes in an arithmetic progression (FOR THE GENERAL MODULUS):

   STATEMENT: Given any two positive integers h, k with $\gcd(h, k) = 1$, there exists at least one prime in the set $\{kn + h\}$, where n ranges over all positive integers.

   Solution:

   One direction of the equivalence is immediate. If there are infinitely many primes in any arithmetic progression (Dirichlet's theorem) then taking the modulus to be k and the residue class to be h, certainly there exists one such prime $p \equiv h\ (k)$, for $\gcd(h, k) = 1$.

   For the reverse direction, assume the statement, and suppose Dirichlet's theorem was false – i.e., there exist some h, k such that there are only finitely many primes $p \equiv h\ (k)$. Then there is a largest one $p_{\max}$. Then consider the arithmetic progression of integers $\equiv h\ (kp_{\max})$. Since h and $kp_{\max}$ are relatively prime, then by the statement, there exists a prime $P \equiv h\ (kp_{\max})$ which implies $P \equiv h\ (k)$ and $P > p_{\max}$, a contradiction.

4. **(BONUS)**

   (a) Prove that $L(1, \chi_q) \neq 0$ if χ_q is a complex character (i.e. $\chi_q(n)$ not real for some n).

   Solution:

   This is straight from the notes. It relies on a proof by contradiction.

   (b) Let χ_q be the non-trivial real character mod q. Choose a prime q and give an explicit evaluation of $L(1, \chi_q)$, thus exhibiting in this special case that the value is non-zero.

   Solution:

   Use the explicit formula for $L(1, \chi_q)$ given for primes $q \equiv 3\ (4)$ to compute an example. (It's just a finite sum so for choice of small q, it is easy to compute explicitly. The example $q = 23$ is done in the notes.