MAT 330 SPRING 2009
REVIEW SESSION 10

1. Review

This week we are preparing ourselves for the proof of the Dirichlet's theorem on primes in arithmetic progressions. The concepts of Dirichlet characters and their associated L-functions were introduced. The factorization of the L-function (in particular, the ζ function) into a product of functions over all primes shows the relevance of these functions in the study of number theory.

2. A little extra

The Dirichlet theorem is about understanding primes in arithmetic progressions. Another question, however, can be asked: are there arbitrarily long arithmetic progressions in the set of all primes? This is a very different question. The answer is yes, and the result was due to Ben Green and Terrence Tao (2004).

In a continuation of this course, MAT 331 (Complex analysis), we shall also study another problem involving the prime numbers, namely the prime number theorem.

3. Discussion of the problem set

In the problem set it was seen that the fact that the discrete Fourier transform on $\mathbb{Z}(N)$ is an isometry was reduced to the fact that a certain matrix M is unitary. In other words, the proof of this fact is really just elementary linear algebra. Recall that the proof of the corresponding statement in the periodic setting, namely the Parseval's identity for Riemann integrable functions on the unit circle, is considerably more difficult. This was because there the space is infinite dimensional, and we needed to take care of issues of convergence by saying that the N-th partial sum of the Fourier series of a Riemann integrable function f provides the best approximation to f among all trigonometric polynomials of degree $\leq N$.

In one other exercise, you were essentially asked to determine which of the groups $\mathbb{Z}(N)^\times$ are cyclic for certain small values of N. It is actually known in general that the group of units mod N is cyclic if and only if $N = 1, 2, 4, p^k$ or $2p^k$ for some odd prime k. A generator of such a group is then called a primitive root $\pmod N$. For those of you who are interested, it is a good exercise to try to prove that every odd prime p has a primitive root. (Hint: use the fact that

$$n = \sum_{d|n} \phi(d)$$

which incidentally is what you're asked to prove in the next problem set.)