Homework #9. Due Wednesday, April 3rd

Reading:

1. For this homework assignment: Chapter 8 and parts of Chapter 7.

2. For the next two classes: Chapter 9 (rough plan is to cover Sections 9.1-9.5)

Problems:

1. Recall that in Exercise 7.20 it was proved that for any $e \geq 1$ there are infinitely many primes of the form $2^e n + 1$, with $n \in \mathbb{N}$, in particular there are infinitely primes of the form $8n + 1$. The goal of this exercise is to use Legendre symbols to prove that there are infinitely many primes of the form $8n+3, 8n+5$ and $8n+7$, thereby completing the proof of Dirichlet's theorem for $a = 8$.
The following facts are (very) relevant for this problem:
(i) If p is an odd prime, the Legendre symbol $\left(\frac{2}{p}\right)$ is equal to 1 if $p \equiv 1$ or 7 mod 8 and is -1 if $p \equiv 3$ or 5 mod 8;
(ii) $x^2 \equiv 1 \mod 8$ for any odd x.

(a) Prove that there are infinitely many primes of the form $8n + 5$. **Hint:** Assume there are only finitely many such primes $p_1, \ldots, p_k$, let $m = 4(p_1 \ldots p_k)^2 + 1$ and show that m has a prime factor of the form $8n + 5$. This is essentially a combination of the methods used to prove that there are infinitely many primes of the form $4n + 3$ and infinitely many primes of the form $4n + 1$, discussed in class.

(b) Now prove that there are infinitely many primes of the form $8n + 7$. **Hint:** Use a trick similar to (a) and (i) and (ii) above.

(c) Finally prove that there are infinitely many primes of the form $8n + 3$. **Hint:** First find an integer $m \in \mathbb{Z}$ such that for any odd prime p we have $\left(\frac{m}{p}\right) = 1 \iff p \equiv 1$ or 3 mod 8.

2. Read about the Jacobi symbol on wikipedia at
`http://en.wikipedia.org/wiki/Jacobi_symbol`

(a) Verify properties 4), 5) and 6) on the wikipedia page.

(b) Prove that if the Jacobi symbol $\left(\frac{a}{n}\right)$ is equal to -1, then a is NOT a quadratic residue mod n.

(c) Give an (explicit) example showing that the Jacobi symbol $\left(\frac{a}{n}\right)$ may equal 1 even when a is not a quadratic residue mod n.

3. Let τ and σ be the functions defined on page 145 of the book. Use multiplicativity of these functions to prove the following results:

(a) $\tau(n)$ is odd $\iff$ n is a perfect square

(b) $\sigma(n)$ is odd $\iff$ n is a perfect square or 2 times a perfect square

4. Let $\mathbb{PP}$ be the set of all prime powers (where 1 is not considered a prime power), and let $f : \mathbb{PP} \to \mathbb{C}$ be an arbitrary function. Extend f to a function $F : \mathbb{N} \to \mathbb{C}$ by setting $f(1) = 1$ and

$$F(p_1^{\alpha_1} \dots p_k^{\alpha_k}) = f({p_1}^{\alpha_1}) \dots f({p_k}^{\alpha_k})$$

whenever $p_1, \dots, p_k$ are distinct primes (so in particular, F restricted to $\mathbb{PP}$ is equal to f). Prove that F is multiplicative.

5. A function $f : \mathbb{N} \to \mathbb{C}$ is called *completely multiplicative* if $f(1) = 1$ and $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$. (Note that the book does not require $f(1) = 1$ in the definition of a multiplicative or completely multiplicative function. However, it is easy to see that the only function which is multiplicative according to the book but does not satisfy $f(1) = 1$ is the zero function).

(a) Formulate and prove the analogue of problem 4 for completely multiplicative functions.

(b) Show by example that the set of completely multiplicative functions is NOT closed under the Dirichlet product $*$

(c) (stronger version of (b)). Let f be a completely multiplicative function different from I (where, as before, $I(1) = 1$ and $I(n) = 0$ for $n > 1$). Prove that $f * f$ is NOT completely multiplicative.

6. Fix an integer $m \geq 1$. As in class, for $n \geq 1$, we denote by A_n the set of all aperiodic words of length n in the alphabet with m symbols. Recall that in class we used Möbius inversion to show that

$$|A_n| = \sum_{d|n} m^d \mu(\frac{n}{d}). \qquad (***)$$

(a) A word w is called l-periodic if $w = v^k$ for some word v of length l (it is not required that v is aperiodic; in other words, the minimal period of w need not be precisely l). Prove that if w is l_1-periodic and l_2-periodic, then it is $gcd(l_1, l_2)$-periodic. **Hint:** To give a clean (yet short) argument, think of w as being written around a circle.

(b) Read about the inclusion-exclusion principle (see Exercise 5.10 in the book or look it up online).

(c) Use the inclusion-exclusion principle to prove the formula (***) above. **Hint:** Given $n \in \mathbb{N}$, let $p_1, \ldots, p_k$ be the distinct prime divisors of n, and apply the inclusion-exclusion principle to the sets $W_{n,n/p_1}, \ldots, W_{n,n/p_k}$ where $W_{n,l}$ is the set of l-periodic words of length n.