Math 437/537 Problem set 5 (due 11/11/09)

Quadratic reciprocity

1. Let p be a prime such that $q = 2p+1$ is also prime. Assuming $p \equiv 3\,(4)$ show that $q|2^p - 1$. Conclude that, with one exception, $2^p - 1$ is not prime.
   Hint: Consider $\left(\frac{2}{q}\right)$.

2. Let χ be the quadratic character $\mod p$. Show that $G(\chi) = \sum_{t=0}^{p-1} \zeta_p^{t^2}$.

Jacobi sums

Let $l_1, \ldots, l_r \geq 1$, let $a_1, \ldots, a_r, b \in \mathbb{Z}$ be non-zero. We will study the equation

$$\sum_{i=1}^{r} a_i x^{l_i} = b\,.$$

3. Let N denote the number of solutions of the equation as a congruence mod p (a prime).
   (a) Assuming p does not divide b nor any of the a_i, express N in the form
   $$N = \sum_{\chi_1,\ldots,\chi_r} C(\chi_1,\ldots,\chi_r) \cdot J(\chi_1,\ldots,\chi_r)$$
   where the summation ranges over certain r-tuples of characters and the coefficients C have modulus 1.
   (b) Under these assumptions, find integers M_0, M_1 so that
   $$\left|N - p^{r-1}\right| \leq M_0 p^{(r/2)-1} + M_1 p^{(r-1)/2}\,.$$
   (c) Find an upper bound on M_0, M_1 depending only on $\underline{l}$ and conclude that if p is large enough (with an explicit lower bound depending only on $\underline{l}$, $\underline{a}$, b), the congruence has a non-zero solution.
   (d) Show that, if p is large enough, the existence of a solution mod p guarantees a solution mod p^k for all k.

4. Find a simple criterion for the existence of a real solution to the equation.

REMARK. With appropriate assumptions on the l_i and on r, the equation $\sum_{i=1}^{r} a_i x^{l_i} = b$ will have solutions in $\mathbb{Q}$ ("global solutions") iff it has solutions in $\mathbb{R}$ and in $\mathbb{Z}/p^k\mathbb{Z}$ for each p,k ("local solutions"). We have shown that checking whether there are local solutions is a finite process.

Arithmetical Functions

- $I(n) = \left[\frac{1}{n}\right]$, $\varepsilon(n) = 1$, $N(n) = n$.
- $\omega(n) = \#\{p \text{ prime} : p|n\}$ i.e. $\omega(\prod_p p^{e_p}) = \sum_p \min\{e_p, 1\}$ and $\Omega(\prod_p p^{e_p}) = \sum_p e_p$.
- Möbius function $\mu(n) = \begin{cases} (-1)^{\omega(n)} & n \,\square\text{free} \\ 0 & \text{otherwise} \end{cases}$, Liouville function $\lambda(n) = (-1)^{\Omega(n)}$.
- von Mangoldt function $\Lambda(n) = \begin{cases} \log p & n = p^k, k \geq 1 \\ 0 & \text{otherwise} \end{cases}$.
- The divisor function $\tau = d = \sigma_0 = \varepsilon * \varepsilon = \#\{a : a|n\}$ and its generalizations $\sigma = \sigma_1 = \varepsilon * N$ and $\sigma_k = \varepsilon * N^k = \sum_{d|n} d^k$.

DEFINITION. The *Dirichlet convolution* of two arithmetical functions $f, g \colon \mathbb{Z}_{\geq 1} \to \mathbb{C}$ is the arithmetical function

$$(f * g)(n) = \sum_{ab=n} f(a)g(b),$$

where the sum is over all pairs $(a,b) \in \mathbb{Z}^2_{\geq 1}$ such that $ab = n$.

5. Show that $*$ is associative and commutative, and that it is distributive over pointwise addition of functions. Show that I is an identity for the operation.

6. (Multiplicative functions) Let f, g be multiplicative functions.
   (a) Show that $f * g$ is multiplicative as well.
   (b) Say $f(p^k) = g(p^k)$ for all primes p and $k \geq 0$. Show that $f = g$.
   (c) Assuming f is not identically zero, show that $f(1) = 1$.

7. (Möbius inverseion)
   (a) Let f be a non-zero multiplicative function. Show that there exists a multiplicative function f^{-1} so that $f * f^{-1} = I$.
   Hint: Define f^{-1} on prime powers first.
   (b) Conclude that if $f, f * g$ are multiplicative and f is non-zero then so is g.
   (c) Show that $\mu * \varepsilon = I$. Obtain the *Möbius inversion formula*: for any two arithmetical functions F, f we have $F(n) = \sum_{d|n} f(d)$ iff $f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$.
   (d) Show that $\Lambda * \varepsilon = \log$ and hence that $\Lambda(n) = -\sum_{d|n} \mu(d) \log d$.
   Hint: consider $\sum_{d|n} \mu(d) \log \frac{n}{d}$ as well.

8. (The divisor function)
   (a) For each integer $n \geq 1$ show that there exists an integer $k \geq 1$ so that $\tau(nk) = n$.
   (b) Starting with $n_0 \geq 1$ set $n_{i+1} = \tau(n_i)$. Show that if n_0 is composite then some n_i is a perfect square.

9. (Some bounds) In the MathSciNet seminar we discussed the problem of integral values of the function $\frac{\phi(n)+\sigma(n)}{n}$.
   (a) Let $p < q$ be primes and let $n = p^\alpha q^\beta$. Show that $\frac{\varphi(n)+\sigma(n)}{n} = 2 + O(\frac{1}{p^2})$, and conclude that if $\frac{\phi(n)+\sigma(n)}{n}$ is an integer then it is equal to 2.
   (b) Show that there exists a function $f(k)$ so that $\frac{\sigma(n)}{n} \leq f(\omega(n))$ for all n.