Homework - 2

ARITHMETIC FUNCTIONS

1. Let n ∈ N. Define an arithmetic function ρ by ρ(1) = 1 and ρ(n) = 2^r where r = number of distinct prime numbers in the prime factorization of n.

   (a) Prove that ρ is multiplicative but not completely multiplicative.

   (b) Let $f(n) = \sum_{d|n} \rho(d)$.

   If $n = p_1^{a_1} \ldots\ldots p_r^{a_r}$, then find a formula for f(n) in terms of this prime factorization.

2. In class we proved the Mobius inversion formula using the following result:

   Let (m,n) = 1, then each divisor d>0 of mn can be uniquely written as d_1d_2, where $d_1, d_2 > 0$, $d_1| m$, $d_2|n$ and $(d_1, d_2) = 1$ and for each such product d_1d_2 corresponds to a divisor d of mn.

   Prove the above result.

3. Prove the identity:

   $$\mu^2(n) = \sum_{d|n} 2^{w(d)} \mu\left(\frac{n}{d}\right) \quad for\ n \in N,$$

   where w(n) denotes the number of distinct prime numbers dividing n.

PRIMITIVE ROOTS

4. Determine whether 2 is a primitive root modulo 19.

5. Let p, q be primes with p = 2q+1. Let a be an integer. Explain why a is primitive root modulo p if and only if $a^2 \not\equiv 1\ (mod\ p)$ and $a^q \not\equiv 1\ (mod\ p)$.

6. Let p be a prime, let g be a primitive root modulo p, and let k be an integer. Prove that g^k is a primitive root modulo p if and only if gcd(k, p-1) = 1.

PRIMALITY TESTING, CARMICHAEL NUMBERS

7. Find all Carmichael numbers of the form 3pq where $3 < p < q$ are primes.

8. Let p be a prime and assume $p^2|m$. Show that there exists a s.t. $(a, m) = 1$ and $a^p \equiv 1\ mod(m)$, and conclude that there exists c s.t. $(c, m) = 1$ and $c^{m-1} \not\equiv 1\ mod(m)$.

QUADRATIC RECIPROCITY

9. Compute the Legendre Symbol. Show all steps and all results used.

$$\left(\frac{402}{991}\right)$$

Hint: 991 is prime.

10. Determine those odds primes p for which 3 is a quadratic residue and those for which it is not.

Hint: Use reciprocity to write

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$$

To determine the last Legendre symbol, we need to know the value of p modulo 3, and to determine $(-1)^{\frac{p-1}{2}}$ we need to know the value of $\frac{p-1}{2}$ modulo 2, or the value of p modulo 4. Hence consider working with p modulo 12. There are only 4 cases to consider $p \equiv 1,\ 5, 7,\ 11\ mod\ 12$. Consider each case separately.