Howard University Math Department

1. (20 points) Explain which of the following statements are true and why. If false, disprove or give a counterexample.

   (a) The Euler function ϕ is an increasing function: $\phi(m) > \phi(n)$ for any $m > n$.

   (b) If g is a primitive root mod p then all powers of g are also primitive roots mod p.

   (c) If a prime p divides the Fermat number $F_n = 2^{2^n} + 1, n \geq 1$, then $p \equiv 1 \pmod 4$.

   (d) If $n = 2^k, k > 2$, then there is no non-trivial solution for $x^n + y^n = z^n$.

2. (20 points) For each of the following give an example. Explain why your example works.

   (a) A prime p for which 3 is a primitive root.

   (b) A number n that can be written as sum of two squares in two ways. Cannot use 0 as one of the squares!

3. (20 points) The Mobius function $\mu(n)$ is an extremely useful tool in number theory when analyzing divisibility of numbers by primes. It is defined as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & if\ n = p_1 p_2 ... p_k \text{ for distinct primes } p_i \\ 0 & \text{otherwise.} \end{cases}$$

   Show that $\mu(n)$ is multiplicative: If $gcd(m, n) = 1$ then $\mu(mn) = \mu(m)\mu(n)$.

4. (20 points) Prove: Every prime element in any integral domain is also irreducible. Give an example of an integral domain with an irreducible element that is not prime. Verify irreducibility and non-primeness in this example.

5. (20 points) Prove using induction that if $M = p_1 p_2 .... p_m$ where the p_i are primes and $p_i \equiv 1 \pmod 4$, $i = 1, 2, 3, ..., m$, then M is a sum of two squares. You may assume that any prime that is congruent to 1 mod 4 is a sum of two squares.