Math 4150-B, Foundations of Mathematical Proof
SAMPLE EXAM 2

1. Suppose that p and q are both odd primes, and that $q = 4p + 1$. Show that 2 is a primitive root modulo q. (Hint: Consider Euler's Criterion)

2. (a) Suppose that r is a primitive root modulo a prime p. Since $-r$ is also relatively prime to p, it most be some power of r modulo p. Make this explicit, i.e., find an integer a such that $-r \equiv r^a \pmod{p}$.
   (b) Suppose now that p is an odd prime, and assume the notation of part a). Find a simple formula for the order of $-r$ modulo p.

3. Show that a is a primitive root modulo n if it is relatively prime to n and $a^{\varphi(n)/p} \not\equiv 1 \pmod{n}$ for all primes $p|\varphi(n)$.

4. Consider the von Mangoldt function, given by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n \text{ is a positive power of a prime } p, \\ 0 & \text{else.} \end{cases}$$

   (a) Show that the summatory function of Λ is $\sum_{d|n} \Lambda(d) = \log n$.
   (b) Show that

$$\Lambda(n) = -\sum_{d|n} \mu(d) \log d.$$

5. (a) State Lucas' Converse of Fermat's Little Theorem.
   (b) Let $F_n = 2^{2^n} + 1$ denote the n-th Fermat number. Show that if there is an integer x such that $x^{2^{2^n}} \equiv 1 \pmod{F_n}$ and $x^{2^{2^n - 1}} \not\equiv 1 \pmod{F_n}$, then F_n is prime.