

**MATH 571 ANALYTIC NUMBER
THEORY I FALL 2007, PROBLEMS 2**

To be submitted by Monday 10th September

1. Let g be a primitive root modulo p . Prove that no k exists satisfying $g^{k+2} \equiv g^{k+1} + 1 \equiv g^k + 2 \pmod{p}$.

Answer questions 2 and 3 in section 1.1.2 (p. 17).

4. Suppose that $p = 2^m + 1$ is a prime, $p \nmid a$ and a is a quadratic non-residue (i.e., not a quadratic residue) modulo p . Show that a is a primitive root modulo p .