

**MATH 567 INTRODUCTION TO NUMBER
THEORY I, FALL TERM 2003, PROBLEMS 11**

Return by Thursday 20th November

1. Prove that if a belongs to the exponent 3 modulo a prime p , then $1 + a + a^2 \equiv 0 \pmod{p}$, and $1 + a$ belongs to the exponent 6.
2. Find the orders modulo 23 of 2, 3 and 5.
3. Find all the primitive roots of 5, 10, 25.
4. First find a primitive root modulo 17 and then find all primitive roots modulo 17.
5. Suppose that $p = 2^m + 1$ is a prime, $p \nmid a$ and a is a quadratic non-residue (i.e., the congruence $x^2 \equiv a \pmod{p}$ has no solutions) modulo p . Show that a is a primitive root modulo p .