Math 180B - Primitive Roots

1. Let p be an odd prime. Prove that a has order 2 mod p if and only if $p \equiv -1 \pmod{p}$.

2. Prove that a quadratic residue is never a primitive root mod p for p and odd prime. *Recall: a is a quadratic residue mod p if $a \equiv b^2 \pmod{p}$ for some b.*

3. Suppose that a has order h mod p, and that $a\bar{a} \equiv 1 \pmod{p}$. Show that $\bar{a}$ also has order h. Suppose that g is a primitive root mod p and that $a \equiv g^i \pmod{p}$, $0 \leq i < p-1$. Show that $\bar{a} \equiv g^{p-1-i} \pmod{p}$.

4. Show that if g and g' are primitive roots modulo and odd prime p, then gg' is not a primitive root mod p.

5. Let p be a prime such that $q = \frac{1}{2}(p-1)$ is also prime. Suppose that g is an integer satisfying

$$g \not\equiv 0 \pmod{p} \quad \text{and} g \not\equiv \pm 1 \pmod{p} \quad \text{and} g^q \not\equiv 1 \pmod{p}.$$

   Prove that g is a primitive root modulo p.

6. Prove that if a has order 3 modulo a prime p, then $1 + a + a^2 \equiv 0 \pmod{p}$, and that $1 + a$ has order 6.

7. Prove that the sequence $1^1, 2^2, 3^3, \ldots$, considered mod p is periodic with least period $p(p-1)$.