Math 173A - Modular Exponentiation

1. Let p be a prime number. Prove that ord_p has the following properties.

   (a) $ord_p(ab) = ord_p(a) + ord_p(b)$

   (b) $ord_p(a+b) \geq \min\{ord_p(a),\ ord_p(b)\}$.

   (c) If $ord_p(a) \neq ord_p(b)$, then $ord_p(a+b) = \min\{ord_p(a),\ ord_p(b)\}$.

2. Let p be a prime. Show that the only solutions to $x^2 \equiv 1 \pmod{p}$ are $x \equiv \pm 1 \pmod{p}$. Is it important that p is a prime?

3. (a) Let p be a prime. Show that if $p \nmid a$, then a^{p-2} is congruent to the multiplicative inverse of a modulo p.

   (b) Find 17^{-1} modulo 101 using the extended Euclidean algorithm and by computing 17^{99} (mod 101) using the square-and-multiply algorithm.

4. (a) Estimate how many multiplication operations modulo N it takes to compute $g^A \pmod{N}$ using the square-and-multiply algorithm. Computing $a \cdot b \pmod{N}$ given a and b is one multiplication operation.

   (b) Recall that in order to compute $g^A \pmod{N}$, the square and multiply algorithm computes (and stores) each of the numbers

   $$g,\ g^2,\ g^{2^2},\ \ldots,\ g^{2^r},$$

   modulo N, where $A = A_0 + A_1 \cdot 2 + A_2 \cdot 2^2 + \cdots + A_r \cdot 2^r$.