Your Name Goes Here

Math 25
Homework 7

1. The following question arose while students were working on homework 6. Suppose that a is a primitive root modulo the odd prime p, but not a primitive root modulo p^2. Show that a is not a primitive root modulo p^e for all $e \geq 2$. Explain how the following hint is relevant and then prove it. Hint: Show by induction that $a^{(p-1)p^{k-1}} \equiv 1 \pmod{p^{k+1}}$ for all $k \geq 1$.

2. Suppose that the positive integer n has a primitive root, and $\gcd(a, n) = 1$. Show that the congruence
$$x^m \equiv a \pmod{n}$$
is solvable iff $a^{\phi(n)/d} \equiv 1 \pmod{n}$ where $d = \gcd(m, \phi(n))$. If it is solvable, show that there are exactly d solutions modulo n.

3. Analogous to problem 1 on Homework 4, it is straightforward to prove the following result (you may assume its validity): Let a be an integer, and p be an odd prime with $p \nmid a$. Then $x^2 \equiv a \pmod{p}$ is solvable if and only if $x^2 \equiv a \pmod{p^e}$ for all $e \geq 1$. Moreover, all these congruences have the same number of solutions.

   (a) Use Gauss's lemma to compute $\left(\frac{5}{19}\right)$.

   (b) Determine whether the following congruence is solvable, and if so determine the number of solutions
   $$x^2 \equiv 5 \pmod{19^7 \cdot 11^3}$$

4. The following exercise will help you find all square roots of -3 in U_{7^3}. It is certainly possible to find a solution modulo 7 and then "lift" it to one modulo 7^3, but this problem outlines an alternate approach.

   (a) Show that 3 is a primitive root modulo 7^3.

   (b) Find the index of -3 with respect to the primitive root 3.

   (c) Use that information to determine all the solutions to $x^2 \equiv -3 \pmod{7^3}$.

5. What is the analog of Corollary 7.10 for $\left(\frac{-2}{p}\right)$? That is, determine congruence conditions to characterize when $-2 \in Q_p$ for an odd prime p. Make sure you involve $\left(\frac{2}{p}\right)$ as part of your answer.