Worksheet 7

In this exercise, we will show that for every $k \geq 1$, $n = p^k$ has primitive roots.
Remark: $k = 1$ (Shown in class).
Let p be an odd prime.

1. Let g be a primitive root modulo p. Show that $g + np$ is a primitive root modulo p^2 for exactly $p - 1$ values of n modulo p.

   Hints:

   Step 1: Show that $ord_{p^2}(g + np) = p - 1$ or $p(p - 1)$.

   Step 2: $ord_{p^2}(g + np) = p - 1$ only for one of the p possible values of n.

   Hints for Step 1:

   (a) Let $h = ord_{p^2}(g + np)$. Show that $h | p(p - 1)$.

   (b) Show that $g^h \equiv 1 \mod p$ to conclude that $(p - 1)|h$. (In order to show $g^h \equiv 1 \mod p$, use that $(g + np)^h \equiv 1 \mod p^2$)

   (c) Combine (a) and (b) to conclude Step 1.

   Hints for Step 2:

   (a) Let $f(x) = x^{p-1} - 1$; then g is a root of the congruence $f(x) \equiv 0 \mod p$. Show $p \nmid f'(g)$.

   (b) Use the following Theorem (*) we did in the class to conclude that there is a unique root of the form $g + np$ of the congruence

   $$f(x) \equiv 0 \mod p^2.$$

   Theorem *: Let p be a prime, a is a solution of $f(x) \equiv 0 \mod p^k$.

   i. If $p \nmid f'(a)$, then there is precisely one solution b of $f(x) \equiv 0 \mod p^{k+1}$ such that $b \equiv a \mod p^k$. The solution is given by $b = a + p^k t$, where t is the unique solution of $f'(a)t \equiv -f(a)/p^k \mod p$.

   (c) Combine (a) and (b) to conclude Step 2.

2. If g is a primitive root modulo p^2, then show g is a primitive root modulo p^k for all $k \geq 2$.

Hints:

Step 1: It suffices to prove that if g is a primitive root $\mod p^k$, $k \geq 2$, then g is also a primitive root $\mod p^{k+1}$.

Show that $ord_{p^{k+1}} g = p^{k-1}(p-1)$ or $p^k(p-1)$.

Step 2: Show that $ord_{p^{k+1}} g = p^{k-1}(p-1)$ is not possible.

Step 3: Combine Step 1 and Step 2.

Hints for Step 1:

(a) Let $h = ord_{p^{k+1}} g$. Show that $h | p^k(p-1)$.

(b) Show that $g^h \equiv 1 \mod p^k$ to conclude that $p^{k-1}(p-1) | h$.

(c) Combine (a) and (b) to conclude Step 1.