Homework 4 : Due Wednesday, February 22

Problem 1: Let p be an odd prime and let $k \in \mathbb{N}^+$. Let $g \in \mathbb{Z}$ with $\gcd(g, p^k) = 1$. Show that g is a primitive root modulo p^k if and only if

$$g^{\varphi(p^k)/q} \not\equiv 1 \pmod{p^k}$$

for all prime divisors q of $\varphi(p^k)$.

Problem 2: Let p be an odd prime and let $k \in \mathbb{N}^+$.
a. Show that if g is a primitive root modulo p^k, then $g^{\varphi(p^k)/2} \equiv -1 \pmod{p^k}$.
b. Show that if a and b are both primitive roots modulo p^k, then ab is not a primitive root modulo p^k.

Problem 3: On Homework 2, you proved the following two results using elementary techniques. Now use the structure of the groups $U(\mathbb{Z}/p^k\mathbb{Z})$ to solve them.
a. Show that if p is an odd prime and $k \in \mathbb{N}^+$, then $x^2 = 1$ has exactly 2 solutions in $\mathbb{Z}/p^k\mathbb{Z}$.
b. Show that $x^2 = 1$ has exactly 4 solutions in $\mathbb{Z}/2^k\mathbb{Z}$ for all $k \geq 3$.
Note: To use the structure of $U(\mathbb{Z}/p^k\mathbb{Z})$, you should first check that any solution must be an element of this group.

Problem 4: Let p be an odd prime. Show how to use the existence of a primitive root modulo p to prove Wilson's Theorem that $(p-1)! \equiv -1 \pmod{p}$.

Problem 5: Suppose that p is an odd prime and $k \in \mathbb{N}^+$. Let S be the set of primitive roots modulo p^k that are elements of the set $\{1, 2, \ldots, p^k - 1\}$.
a. Show that if $(p, k) \neq (3, 1)$, then product of the elements of S is congruent to 1 modulo p^k.
b. Show that if $k = 2$, then S has exactly $(p-1) \cdot \varphi(p-1)$ many elements.

Problem 6: Let p be an odd prime and let $m \in \mathbb{N}^+$. Let $d = \gcd(p-1, m)$.
a. Show that there are exactly d solutions to $x^m = 1$ in $\mathbb{Z}/p\mathbb{Z}$.
b. Define $\psi \colon U(\mathbb{Z}/p\mathbb{Z}) \to U(\mathbb{Z}/p\mathbb{Z})$ by letting $\psi(x) = x^m$. Show that $|\text{range}(\psi)| = \frac{p-1}{d}$. In other words, show that there are exactly $\frac{p-1}{d}$ many m^{th} powers in $\mathbb{Z}/p\mathbb{Z}$ (excluding $\overline{0}$).
Hint for b: Start by show that ψ is a group homomorphism.