Number Theory Homework #5

1. Let $g$ be a primitive root modulo $m$. Prove that $g^k$ is a primitive root modulo $m$ if and only if $\gcd(k, \varphi(m)) = 1$. Deduce that if there exists a primitive root modulo $m$, then the number of primitive roots modulo $m$ is $\varphi(\varphi(m))$.

2. (a) Show that 2 is a primitive root modulo 29.
(b) Compute all primitive roots for $p = 11, 13, 17, \text{and} 19$.

3. (a) Find the four primitive roots modulo 26 and the eight primitive roots modulo 25.
(b) Determine all the primitive roots modulo $3^2, 3^3, \text{and} 3^4$.

4. (a) Prove that 3 is a primitive root for all integers of the form $7^k$ and $2 \cdot 7^k$.
(b) Find a primitive root for any integer of the form $17^k$.

5. Prove that if $p$ and $q = 2p + 1$ are both odd primes (for example $p = 5$ and $q = 11$), then $-4$ is a primitive root mod $q$.

6. Show that 4 is not a primitive root modulo $n$ for any $n \geq 2$.

7. Let $p \geq 3$ be a prime number, let $r \in \mathbb{N}$, and let $x$ be a primitive root modulo $p^r$. Show that $x$ is a primitive root modulo $p$. 