Worksheet 8: Primitive Roots

1. Compute all primitive roots mod 6, 7, and 8.

2. Suppose $a$ has order $n$ mod $m$, and $a^k \equiv 1 \mod m$. Show that $n|k$.

3. Show that, if $a$ is a primitive root mod $m$, then $\{a, a^2, \ldots, a^{\phi(m)}\}$ is a reduced residue system mod $m$.

4. Suppose $a$ has order $n$ mod $m$, and $\gcd(k, n) = g$. Show that $a^k$ has order $\frac{n}{g}$ mod $m$. Conclude that this implies the following two corollaries:
   
   (a) If $a$ is a primitive root mod $m$, then $a^k$ is also a primitive root mod $m$ if and only if $\gcd(k, \phi(m)) = 1$.
   
   (b) If there exists a primitive root mod $m$, then there are precisely $\phi(\phi(m))$ primitive roots.

5. Andrews 7.1.6, 7.2.15, Stein 2.8, 2.30.

6. Write down a precise statement for each definition we have given this week. For each definition, give an example and a non-example.