SOLUTIONS: PROBLEM SET 20 FROM SECTION 9.2

2.

(a) 5 and 8 are roots.
(b) 12 and 11 are roots.
(c) 1,3 and 9 are roots.
(d) 6 is the only root.

6. 3,5,6,7,10,11,12,14.

12. If a is a primitive root $\pmod p$, then so is $\bar{a}$, where $\bar{a}$ is a modular inverse of a, $\pmod p$. Moreover if $\bar{a} \equiv a \pmod p$, then $a^2 \equiv 1 \pmod p$, in which case $a \equiv \pm 1 \pmod p$. This last is the case if $p = 2$, $a = 1$, or $p = 3$, $a = 2$. In all other cases, the product of the primitive roots breaks up into a product of products of the form $a\bar{a}$, and so has the least positive residue 1. This is true also if $p = 2$, in which case the only primitive root is 1. The only exception, therefore, is $p = 3$ for which the product of the primitive roots is the unique primitive root 2.