Math 435 Number Theory I
Problem Set 9

Due: Friday November 4

1) Prove that 7 is a primitive root in U_{71}.

2) 5 is a primitive root in U_{23}. Below is a table of powers of 5 mod 23.

n	1	2	3	4	5	6	7	8	9	10	11
5^n	5	2	10	4	20	8	17	16	11	9	22

n	12	13	14	15	16	17	18	19	20	21	22
5^n	18	21	13	19	3	15	6	7	12	14	1

For each of the following equations. Decide if there is a solution in $\mathbb{Z}_{23}$. If so find all solutions.

a) $X^8 \equiv 13 \pmod{23}$.
b) $X^8 \equiv 14 \pmod{23}$.
c) $X^5 \equiv 21 \pmod{23}$.

3) Let $n > 1$. Suppose g is a primitive root mod n. Develop an easy rule for determining for which k, g^k is a primitive root. Prove that your rule is correct.

4) a) Suppose $a = b^2$ and $n > 2$. Prove that a is not a primitive root mod n.
b) Is the same thing true if, instead, we assume $a = b^3$?