1. Which of the following integers have primitive roots: 4, 10, 16, 22, 28?

2. Show that if m is a positive integer without a primitive root, then there exists a solution to the congruence $x^2 \equiv 1 \mod m$ so that $x \not\equiv \pm 1 \mod m$. Note that this is the converse to problem 4 on homework 5.
   Hint: Recall that you previously showed that $x^2 \equiv 1 \mod 2^e$ has four solutions when $e \geqslant 3$.

3. Find all solutions to the following congruence: $3x^5 \equiv 1 \mod 23$. You may use the fact that 5 is a primitive root modulo 23.

4. Let m be a positive integer with primitive root r and let $a, b \in (\mathbb{Z} / m\mathbb{Z})^{\times}$. Show the following and give an example showing that equality does not always hold.

   (a) $\operatorname{ind}_r(1) \equiv 0 \mod \varphi(m)$

   (b) $\operatorname{ind}_r(ab) \equiv \operatorname{ind}_r(a) + \operatorname{ind}_r(b) \mod \varphi(m)$

   (c) $\operatorname{ind}_r(a^k) \equiv k \operatorname{ind}_r(a) \mod \varphi(m)$

5. Let p be an odd prime. Show that every element of $(\mathbb{Z}/p\mathbb{Z})^\times$ is a pth power residue.

Homework Draft Problems

Note: I will probably choose 4 of these to assign for homework.

1. Suppose that m has a primitive root. Show that the product of all elements of $(\mathbb{Z}\,/\,m\mathbb{Z})^\times$ is congruent to -1 mod m.
   Hint: This reduces to Wilson's Theorem when m is prime.
2. For which positive integers a is the congruence $ax^4 \equiv 2 \mod 13$ solvable?
3. Find all solutions of $x^x \equiv x \mod 23$
4. Let $N = 2^j u$ be a positive integer where $j \geqslant 0$ and u is odd. Let p be an odd prime and factor $p - 1 = 2^s t$ where s and t are positive integers with t odd. Show that if $0 \leqslant j < s$, then there are $2^j (t, u)$ incongruent solutions of $x^N \equiv -1 \mod p$. Show that there are no solutions otherwise.
5. In class, we found a way of checking to see if a is a kth power residue modulo any m as long as m has a primitive root. Large enough powers of 2, however, do not have primitive roots. In this problem, suppose that k is even. Show that an integer a is a kth power residue modulo 2^e if and only if $a \equiv 1 \mod (4k, 2^e)$ when $e \geqslant 2$.