1. *Suppose that $m > 2$ 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.

By problem 4 on Homework 5, we know that the only solutions to $x^2 \equiv 1 \mod m$ are $x \equiv \pm 1 \mod m$. Hence, the only elements of $(\mathbb{Z}/m\mathbb{Z})^\times$ that are self-inverse are $x \equiv \pm 1 \mod m$. Therefore, every $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ with $a \not\equiv \pm 1 \mod m$ can be paired with its multiplicative inverse a^{-1} and we have:

$$\prod_{n \in (\mathbb{Z}/n\mathbb{Z})^\times} n \equiv (1)(-1)a_1 a_1^{-1} \cdots a_{\frac{\varphi(m)}{2}-1} a_{\frac{\varphi(m)}{2}-1}^{-1} \equiv -1 \mod m$$

Alternate Solution

Suppose that r is a primitive root of m. Then for every $n \in (\mathbb{Z}/m\mathbb{Z})^\times$ there exists a unique integer k satisfying $1 \leqslant k \leqslant \varphi(m)$ so that $n \equiv r^k \mod m$. Hence,

$$\prod_{n \in (\mathbb{Z}/m\mathbb{Z})^\times} n \equiv \prod_{k=1}^{\varphi(m)} r^k \equiv r^{\sum_{k=1}^{\varphi}(m)k} \equiv r^{\frac{\varphi(m)\cdot(\varphi(m)+1)}{2}} \equiv \left(r^{\varphi(m)/2}\right)^{\varphi(m)+1} \mod m$$

By the proof of problem 4 on Homework 5, we have $r^{\varphi(m)/2} \equiv -1 \mod m$. Moreover, $\varphi(m)+1$ is odd and so

$$\prod_{n \in (\mathbb{Z}/m\mathbb{Z})^\times} \equiv \left(r^{\varphi(m)/2}\right)^{\varphi(m)+1} \equiv (-1)^{\varphi(m)+1} \equiv -1 \mod m$$

2. *Suppose that m has a primitive root, r. Show that $a \equiv b \mod m$ if and only if* $\operatorname{ind}_r(a) \equiv \operatorname{ind}_r(b) \mod \varphi(m)$.
Note: This shows that "taking indices is invertible."

   If $a \equiv b \mod m$, then the unique x satisfying $1 \leqslant x \leqslant \varphi(m)$ so that $r^x \equiv a \mod m$ also has $r^x \equiv b \mod m$. Hence, $\operatorname{ind}_r(a) \equiv \operatorname{ind}_r(b) \mod \varphi(m)$.

   Likewise, if $\operatorname{ind}_r(a) \equiv \operatorname{ind}_r(b) \mod \varphi(m)$ then

$$a \equiv r^{\operatorname{ind}_r(a)} \equiv r^{\operatorname{ind}_r(b)} \equiv b \mod m$$

3. *For which positive integers a is the congruence $ax^4 \equiv 2 \mod 13$ solvable?*

By the previous problem together with the fact that 2 is a primitive root modulo 13, there exists an x so that $ax^4 \equiv 2 \mod 13$ if and only if

$$\operatorname{ind}_2(ax^4) \equiv \operatorname{ind}_2(2) \mod 12$$

This is equivalent to the claim that

$$\operatorname{ind}_2(a) + 4\operatorname{ind}_2(x) \equiv 1 \mod 12$$

which is then equivalent to the claim that

$$4\operatorname{ind}_2(x) \equiv 1 - \operatorname{ind}_2(a) \mod 12$$

By theorem 4.11, the above equation has solutions if and only if $4 = (4, 12) \mid 1 - \operatorname{ind}_2(a)$, i.e. $\operatorname{ind}_2(a) \equiv 1 \mod 4$. The only integers between 1 and 12 which are congruent to 1 mod 4 are 1, 5, and 9, so we have solutions to $ax^4 \equiv 2 \mod 13$ if and only if $\operatorname{ind}_2(a) \equiv 1, 5, 9 \mod 12$, i.e. $a \equiv 2, 2^5, 2^9 \mod 13$.

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.*

   Since p is a prime, p has a primitive root, say r. Then by problem 2 on this assignment, $x^N \equiv -1 \mod p$ has a solution if and only $N \operatorname{ind}_r(x) \equiv \operatorname{ind}_r(-1) \mod p - 1$ has a solution.

   Note that since r is a primitive root, by problem 1 on homework 5, $\operatorname{ind}_r(-1) = \frac{p-1}{2} = 2^{s-1}t$. Hence, we have a solution to $x^N \equiv -1 \mod p$ if and only if $N \operatorname{ind}_r(x) \equiv 2^{s-1}t \mod 2^s t$ has a solution. But this linear equation has a solution if and only if $(N, 2^s t) \mid 2^{s-1}t$ (again using Theorem 4.11). However,

$$(N, 2^s t) = (2^j u, 2^s t) = 2^{\min(j,s)} \cdot (2^{j-\min(j,s)} u, 2^{s-\min(j,s)} t) = 2^{\min(j,s)}(u, t)$$

   Now, $2^{\min(j,s)}(u, t) \mid 2^{s-1}t$ if and only if $j < s$ meaning that there are solutions to $N \operatorname{ind}_r(x) \equiv 2^{s-1}t \mod 2^s t$ if and only if $j < s$. In the case that $j < s$, there are $(N, 2^s t) = 2^j(u, t)$ solutions.