1) Show that 2 is a primitive root modulo 11.

A number is a primitive root modulo a prime p if its multiplicative order modulo p is $\varphi(p) = p-1$. Here p is 11, so we need to check that the order of 2 mod 11 is 10.

Let us compute successive power of 2 mod 11:

$2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 5$, $2^5 \equiv 10$, $2^6 \equiv 9$, $2^8 \equiv 14 \equiv 3$, $2^9 = 6$
$2^{10} \equiv 12 \equiv 1$. (mod 11)

No smaller positive exponent gives 1 modulo 11 so the order of 2 is 10 $= \varphi(11)$. Hence 2 is a primitive root modulo 2.

2) How many incongruent primitive roots does 14 have?

Soln: If primitive roots exist modulo n, their number equal $\varphi(\varphi(n))$.
First compute $\varphi(14)$. Since $14 = 2 \cdot 7$, $\varphi(14) = \varphi(2) \cdot \varphi(7) = 1 \cdot 6 = 6$.
Thus the primitive root if it exists, is $\varphi(\varphi(6)) = 2$.
(Primitive roots do exist where p is an odd prime number). So the formula applies.
The units modulo 14 are $\{1, 3, 5, 9, 11, 13\}$. A element is primitive if it has 6. Checking for 3: $3^1 = 3$, $3^2 \equiv 9$, $3^3 \equiv 13$, $3^4 \equiv 11$, $3^5 \equiv 5$. $3^6 \equiv 1$ (mod 14)
So 3 has order 6. It's inverse 5 (since $3 \cdot 5 \equiv 1$) is the other root. So the two incongruent pritive roots modulo 14 are 3 and 5.

3. Suppose n is a positive integer and $\bar{a}^1$ is a multiplicative inverse of $a \pmod n$.

a. Show that $\mathrm{ord}_n a = \mathrm{ord}_n(\bar{a}^{1})$

b. If a is a primitive root modulo n, must $\bar{a}^1$ also be a primitive root.

Soln:

(a). Let $m = \mathrm{ord}_n(a)$. By definition $a^m \equiv 1 \pmod n$ and m is the least positive integer with that property. Raise inverse to the same power:

$$\bar{a}^1(m) \equiv (a^m)^{-1} \equiv 1^{-1} \equiv 1 \pmod n,$$

so $\mathrm{ord}_n(\bar{a}^1)$ divides m. conversely, if $(\bar{a}^1)^k \equiv 1 \pmod n$ then taking inverses gives $a^k \equiv 1 \pmod n$, so m divides k. Hence the least positive exponent of $\bar{a}^1$ equals m. Therefore $\mathrm{ord}_n(\bar{a}^1) = \mathrm{ord}_n(a)$

An equivalent short argument: since $a^m \equiv 1$, we have $\bar{a}^1 \equiv a^{m-1}$, so $\bar{a}^1$ is a power of a; powers of an element have the same order as the element when the exponent is ~~invert~~ invertible modulo the order. Here the minimality argument above is simplest and direct.

b) Yes, If a is a primitive root modulo n then $\mathrm{ord}_n(a) = \phi(n)$. By part (a) $\mathrm{ord}_n(\bar{a}^1) = \mathrm{ord}_n(a) = \phi(n)$, so $\bar{a}^1$ is also a primitive root.