1. Let $n > 1$ and let $a$ be an integer coprime to $n$. Let $a^{-1}$ denote the multiplicative inverse of $a$ modulo $n$.

(a) Let $j \geq 1$. Show that $a^j \equiv 1 \bmod n \iff (a^{-1})^j \equiv 1 \bmod n$.

(b) Use part (a) to show that the order of $a$ is the same as the order $a^{-1}$.

(a) If $a^j \equiv 1 \bmod n$, then multiplying both sides by $(a^{-1})^j$, we get $1 \equiv (a^{-1})^j \bmod n$.
If $(a^{-1})^j \equiv 1 \bmod n$, then multiply both sides by $a^j$ to get $1 \equiv a^j \bmod n$.

(b) By part (a), we have $\{j \geq 1 : a^j \equiv 1 \bmod n\} = \{j \geq 1 : (a^{-1})^j \equiv 1 \bmod n\}$. Since the sets are the same, the least element of both sets is the same. Thus the order of $a$ mod $n$ is the same as the order of $a^{-1}$ mod $n$.

2. (a) List all the positive integers less than or equal to 14 which are relatively prime to 14.

(b) Find the order mod 14 of each integer in your list from part (b). Show your work.

(c) Using your answer to part (c), list all the primitive roots of 14 (if any).

(d) The number of primitive roots you found in part (c) should be $\phi(\phi(14))$. Confirm that this is true.

(a) $1, 3, 5, 9, 11, 13$.

(b) The order of any element must divide $\phi(14) = 6$. So the possible orders are $1, 2, 3$, or $6$.

The order of 1 is 1, because $1^1 \equiv 1 \bmod 14$.
The order of 3 is 6, because $3^1 \equiv 3 \bmod 14, 3^2 \equiv 9 \bmod 14, 3^3 \equiv -1 \bmod 14$.
The order of 5 is 6, because $5^1 \equiv 5 \bmod 14, 5^2 \equiv -3 \bmod 14, 5^3 \equiv -1 \bmod 14$.
The order of 9 is 3, because $9^1 \equiv -5 \bmod 14, 9^2 \equiv -3 \bmod 14, 9^3 \equiv 1 \bmod 14$.
The order of 11 is 3, because $11^1 \equiv -3 \bmod 14, 11^2 \equiv 9 \bmod 14, 11^3 \equiv 1 \bmod 14$.
The order of 13 is 2, because $13^1 \equiv -1 \bmod 14, 13^2 \equiv 1 \bmod 14$.

(c) 3 and 5

(d) $\phi(\phi(14)) = \phi(6) = 2$. Yes, we found two primitive roots in part (c).

3. Show that any odd prime divisor $p$ of $n^4 + 1$ must be of the form $p = 8k + 1$.

Suppose that $n^4 + 1$ has an odd prime divisor $p$. Then $n^4 + 1 \equiv 0 \bmod p$. This implies $n^4 \equiv -1 \bmod p$, which implies $n^8 \equiv 1 \bmod p$. So the order of $n$ divides 8, which means that the order is $1, 2, 4$ or 8. The order cannot be $1, 2$, or 4 because otherwise $n^4 \equiv 1 \bmod p$ and this would contradict $n^4 \equiv -1 \bmod p$ as $p \neq 2$. Thus the order of $n$ is 8. The order of an integer mod $m$ must divide $\phi(m)$, so 8 must divide $\phi(p) = p - 1$. This means $p - 1 = 8k$, or equivalently, $p = 1 + 8k$.

4. Given that 3 is a primitive root mod 17, list all the primitive roots mod 17 using suitable powers of 3. There should be eight of them, including 3.

The order of 3 mod 17 is $\phi(17) = 16$. The order of $3^h$ is $\frac{16}{(16,h)}$. Thus the order of $3^h$ is 16 if and only if $(16, h) = 1$. List the positive integers less than or equal to 16 with order coprime to 16:

$$1, 3, 5, 7, 9, 11, 13, 15.$$

Thus the primitive roots mod 17 are:

$3^1 \equiv 3 \bmod 17$
$3^3 \equiv 10 \bmod 17$
$3^5 \equiv 5 \bmod 17$
$3^7 \equiv 11 \bmod 17$
$3^9 \equiv 14 \bmod 17$
$3^{11} \equiv 7 \bmod 17$
$3^{13} \equiv 12 \bmod 17$
$3^{15} \equiv 6 \bmod 17$