

Q3a: We will prove the contrapositive. If a is odd, then we have that a^m is also odd, for any $m \in \mathbb{N}$. Therefore, $a^m + 1$ is even, and it has factors. Now, if m is a power of 2, we can write it as $m = 2^n \cdot q$ for some odd q . Consider the polynomial $f(t) = t^q + 1$. This polynomial has a root $t = -1$ and thus it splits. Letting $t = x^{2^n}$, we see that $g(x) = f(x^{2^n}) = x^m + 1$ has a proper factor x^{2^n} . Letting $x = a$ we see that $a^{2^n} + 1$ is a proper factor of $a^m + 1$ thus it cannot be prime.

Q3b: First suppose that $a > 2$. Then we have that $a^m - 1 = (a - 1)(a^{m-1} + a^{m-2} + \cdots + 1)$. Therefore, $a - 1 \mid a^m - 1$. Since $(a - 1) > 1$ we have that $a^m - 1$ is composite. Therefore $a = 2$. Now suppose that m is not prime. Therefore, $m = qp$ for some $q, p \neq 1$. Then we have that

$$\begin{aligned} a^m - 1 &= a^{pq} - 1 \\ &= a^{p^q} - 1 \\ &= (a^p - 1)(a^{p^{q-1}} + a^{p^{q-2}} + \cdots + a^p + 1) \end{aligned}$$

Thus $(a^p - 1) \mid (a^m - 1)$. Thus it can not be prime. Therefore if $m > 1$ and $a^n - 1$ is prime, $a \geq 2$ and m is prime.