QUESTION

Let $p = a^m + 1$ be a prime, where $a \geq 2$ and $m \geq 1$ are integers. Prove that a must be even and $m = 2^n$ for some positive integer, n.

ANSWER

If q is odd then we have the following identity between polynomials with integral coefficients

$$t^q + 1 = (t+1)(t^{q-1} - t^{q-2} + \ldots - t + 1).$$

For our purposes it would be sufficient to know that $t+1$ divides $t^q + 1$ in $Z[t]$. Now write $m = 2^n q$ where q is odd. Setting $t = a^{2^n}$ yields

$$t^q + 1 = (a^{2^n})^q + 1 = a^{2^n q} + 1 = p.$$

Therefore $a^{2^n} + 1$ divides p in the integers. However, $2 \leq a^{2^n} + 1$ for all n and $a^{2^n} + 1 = p$ if and only if $q = 1$. Hence p has proper divisors unless $n = 2^n$. Even so, for any m, p would be even if a were odd, so a must be even.