Proof of divisibility by 3

Pixelwitch

June 21, 2016

Let it be true for $n = k$ that $2^{2n} - 1$ is divisible by 3 This implies that as

$$2^{2k} - 1 = (2^k - 1)(2^k + 1)$$

Either $(2^k - 1)$ is divisible by 3, or $(2^k + 1)$ is divisible by 3. And hence

$$2^k = 3m + 1 \quad \text{or} \quad 2^k = 3m - 1$$

Where $m \in \mathbb{N}$.

As this is true for $n = k$, if it were the case that for $n = k$, $2^k = 3m + 1$

$$\begin{aligned} 2^{2(k+1)} - 1 &= (2^{k+1} - 1)(2^{k+1} + 1) \\ &= (2^k \times 2 - 1)(2^k \times 2 + 1) \\ &= (2(3m + 1) - 1)(2(3m + 1) + 1) \\ &= (6m + 1)(6m + 3) \\ &= 3(6m + 1)(2m + 1) \end{aligned}$$

$$\frac{3(6m + 1)(2m + 1)}{3} = (6m + 1)(2m + 1) \in \mathbb{N}.$$

In the alternative case, that for $n = k$, $2^k = 3m - 1$

$$\begin{aligned} 2^{2(k+1)} - 1 &= (2^{k+1} - 1)(2^{k+1} + 1) \\ &= (2^k \times 2 - 1)(2^k \times 2 + 1) \\ &= (2(3m - 1) - 1)(2(3m - 1) + 1) \\ &= (6m - 3)(6m - 1) \\ &= 3(2m - 1)(6m - 1) \end{aligned}$$

$$\frac{3(2m - 1)(6m - 1)}{3} = (2m - 1)(6m - 1) \in \mathbb{N}.$$

Hence it is true for either case arising in $n = k$, and hence for $n = k + 1$.
For $n = 1$

$$\begin{aligned} 2^{2(1)} - 1 &= 4 - 1 \\ &= 3 \end{aligned}$$

$$\frac{3}{3} = 1 \in \mathbb{N}.$$

Which makes it true for $n = 1$. As it is true for $n = 1$ and $n = k+1$, by the principle of mathematical induction it is true for all $n \geq 1$