2018 TSTST #8

Tristan Shin

4 July 2018

For which positive integers $b > 2$ do there exist infinitely many positive integers n such that n^2 divides $b^n + 1$?

The answer is $\boxed{b \text{ such that } b+1 \text{ is not a power of } 2}$.

Suppose $b+1$ is a power of 2, say $b+1 = 2^k$ with $k \geq 2$. If $n^2 \mid b^n + 1$, with n not a power of 2, then let p be the smallest odd divisor of n. Then

$$p \mid n^2 \mid b^n + 1 \mid b^{2n} - 1,$$

so $\operatorname{ord}_p b \mid (2n, p-1) = 2$. If $\operatorname{ord}_p b = 1$, then $p \mid b - 1$, so $p \mid 2$, contradiction. So $\operatorname{ord}_p b = 2$ and thus $p \mid b + 1 = 2^k$, contradiction. So n must be a power of 2, say $n = 2^j$ with $j \geq 1$ ($n = 1$ trivially works). Then $b \equiv -1 \pmod 4$, so $b^n \equiv 1 \pmod 4$, but $b^n + 1 \equiv 0 \pmod 4$, contradiction. Thus, $b+1$ is not a power of 2.

Now, assume that $b+1$ is not a power of 2. We will inductively define a sequence of odd primes $p_0, p_1, p_2, \ldots$ such that

$$\begin{gathered}(p_0 p_1 \cdots p_{i-1})^2 p_i \mid b^{p_0 p_1 \cdots p_{i-1}} + 1 \\ (p_0 p_1 \cdots p_i)^2 \mid b^{p_0 p_1 \cdots p_i} + 1\end{gathered}$$

for all $i = 0, 1, 2, \ldots$.

Let p_0 be any odd prime dividing $b+1$. Then by LTE,

$$v_{p_0}\left(b^{p_0} + 1\right) = v_{p_0}(b+1) + v_{p_0}(p_0) \geq 2,$$

so $p_0^2 \mid b^{p_0} + 1$. Now, assume that $p_0, p_1, \ldots, p_i$ have been defined and satisfy the conditions. Let p_{i+1} be a prime dividing $b^{p_0 p_1 p_2 \cdots p_i} + 1$ but not $b^e + 1$ for $e < p_0 p_1 p_2 \cdots p_i$ (possible by Zsigmondy). Then $p_{i+1} \neq p_j$ for $j = 0, 1, 2, \ldots, i$ because $p_0 p_1 \cdots p_i \mid b^{p_0 p_1 \cdots p_{i-1}} + 1$, so

$$(p_0 p_1 \cdots p_i)^2 p_{i+1} \mid b^{p_0 p_1 \cdots p_i} + 1.$$

Furthermore,

$$v_{p_{i+1}}\left(b^{p_0 p_1 \cdots p_i p_{i+1}} + 1\right) = v_{p_{i+1}}\left(b^{p_0 p_1 \cdots p_i} + 1\right) + v_{p_{i+1}}(p_{i+1}) \geq 2$$

by LTE, so

$$(p_0 p_1 \cdots p_{i+1})^2 \mid b^{p_0 p_1 \cdots p_{i+1}} + 1.$$

Thus, we have constructed this sequence of primes. Then

$$p_0, p_0 p_1, p_0 p_1 p_2, p_0 p_1 p_2 p_3, \ldots$$

is an infinite sequence of positive integers n such that n^2 divides $b^n + 1$, so we are done. ■