Bilkent University
Department of Mathematics

Problem Of The Month

January 2016

Problem:

Find all positive integer numbers n such that for any positive integer a relatively prime to n the number $2n^2$ divides $a^n - 1$.

Solution:

Let $p > 2$ be a prime divisor of n (if any) and let p^m be the greatest power of p that divides n: $v_p(n) = m$. Let us choose a such that $a \equiv p+1 \pmod{p^2}$ and $a \equiv 1 \pmod{\frac{n}{p^m}}$. Since $p \mid a-1$, one gets $v_p(a^n - 1) = v_p(a-1) + v_p(n) = m+1$. But $a^n - 1$ is divisible by n^2, so $m + 1 \geq 2m \Rightarrow m \leq 1 \Rightarrow m = 1$. Now let 2^m be the greatest power of 2 that divides n. Choose a such that $a \equiv 5 \pmod 8$ and $a \equiv 1 \pmod{\frac{n}{2^m}}$. Since $4 \mid a-1$, one gets $v_2(a^n - 1) = v_2(a-1) + v_2(n) = m + 2$. Much like the same way as above, $m + 2 \geq 2m + 1 \Rightarrow m \leq 1$. Thus, n is a square-free integer.

Now let p be any prime divisor of n and choose a such that it is congruent to a primitive root $\pmod p$ and congruent to $1 \pmod{\frac{n}{p}}$. Since $p \mid a^n - 1$, one gets $p - 1 \mid n$. In other words, $p \mid n$ implies $p - 1 \mid n$. It is also easy to see that this condition together with the square-freeness of n is sufficient for the original condition to be true. Let $n = p_1 \cdot p_2 \cdots p_k$ (we assume $p_1 < p_2 < \ldots < p_k$). For each i, one has $p_i - 1 \mid n \Rightarrow p_i - 1 \mid p_1 \cdot p_2 \cdots p_{i-1}$. Since $n = 1$ obviously doesn't satisfy the problem condition, $k \geq 1$.
As such, $p_1 - 1 \mid 1 \Rightarrow p_1 = 2$.
For $i = 2$, $p_2 - 1 \mid p_1 = 2$ and $p_2 > p_1 = 2$, therefore $p_2 = 3$.
For $i = 3$, $p_3 - 1 \mid p_1 \cdot p_2 = 6$ and $p_3 > p_2 = 3$, therefore $p_3 = 7$.
For $i = 4$, $p_4 - 1 \mid p_1 \cdot p_2 \cdot p_3 = 42$ and $p_4 > p_3 = 7$, therefore $p_4 = 43$.
For $i = 5$, $p_5 - 1 \mid p_1 \cdot p_2 \cdot p_3 \cdot p_4 = 1806$ and $p_5 > p_4 = 43$, which is impossible ($1807 = 13 \cdot 139$) so $k \leq 4$.
Thus, the possible values of n are: $2, 6, 42, 1806$.