USEMO 2021/2

Evan Chen

Twitch Solves ISL

Episode 89

Problem

Find all integers $n \geq 1$ such that $2^n - 1$ has exactly n positive integer divisors.

Video

https://youtu.be/V-9UBJr7aDI

Solution

The valid n are 1, 2, 4, 6, 8, 16, 32. They can be verified to work through inspection, using the well known fact that the Fermat prime $F_i = 2^{2^i} + 1$ is indeed prime for $i = 0, 1, \dots, 4$ (but not prime when $i = 5$).

We turn to the proof that these are the only valid values of n. In both solutions that follow, $d(n)$ is the divisor counting function.

First approach (from author) Let d be the divisor count function. Now suppose n works, and write $n = 2^k m$ with m odd. Observe that

$$2^n - 1 = (2^m - 1)(2^m + 1)(2^{2m} + 1) \cdots (2^{2^{k-1}m} + 1),$$

and all $k + 1$ factors on the RHS are pairwise coprime. In particular,

$$d(2^m - 1)d(2^m + 1)d(2^{2m} + 1) \cdots d(2^{2^{k-1}m} + 1) = 2^k m.$$

Recall the following fact, which follows from Mihăilescu's theorem.

Lemma. $2^r - 1$ is a square if and only if $r = 1$, and $2^r + 1$ is a square if and only if $r = 3$.

Now, if $m \geq 5$, then all $k + 1$ factors on the LHS are even, a contradiction. Thus $m \leq 3$. We deal with both cases.

If $m = 1$, then the inequalities

$$\begin{aligned} d(2^{2^0} - 1) &= 1 \\ d(2^{2^0} + 1) &\geq 2 \\ d(2^{2^1} + 1) &\geq 2 \\ &\vdots \\ d(2^{2^{k-1}} + 1) &\geq 2 \end{aligned}$$

mean that it is necessary and sufficient for all of $2^{2^0} + 1,\ 2^{2^1} + 1,\ \dots,\ 2^{2^{k-1}} + 1$ to be prime. As mentioned at the start of the problem, this happens if and only if $k \leq 5$, giving the answers $n \in \{1, 2, 4, 8, 16, 32\}$.

If $m = 3$, then the inequalities

$$\begin{aligned} d(2^{3 \cdot 2^0} - 1) &= 2 \\ d(2^{3 \cdot 2^0} + 1) &= 3 \\ d(2^{3 \cdot 2^1} + 1) &\geq 4 \\ &\vdots \\ d(2^{3 \cdot 2^{k-1}} + 1) &\geq 4 \end{aligned}$$

mean that $k \geq 2$ does not lead to a solution. Thus $k \leq 1$, and the only valid possibility turns out to be $n = 6$.

Consolidating both cases, we obtain the claimed answer $n \in \{1, 2, 4, 6, 8, 16, 32\}$.

Second approach using Zsigmondy (suggested by reviewers) There are several variations of this Zsigmondy solution; we present the approach found by Nikolai Beluhov. Assume $n \ge 7$, and let $n = \prod_1^m p_i^{e_i}$ be the prime factorization with $e_i > 0$ for each i. Define the numbers

$$\begin{aligned} T_1 &= 2^{p_1^{e1}} - 1 \\ T_2 &= 2^{p_2^{e2}} - 1 \\ &\vdots \\ T_m &= 2^{p_m^{em}} - 1. \end{aligned}$$

We are going to use two facts about T_i.

Claim. The T_i are pairwise relatively prime and

$$\prod_{i=1}^{m} T_i \mid 2^n - 1.$$

Proof. Each T_i divides $2^n - 1$, and the relatively prime part follows from the identity $\gcd(2^x - 1, 2^y - 1) = 2^{\gcd(x,y)} - 1$. □

Claim. The number T_i has at least e_i distinct prime factors.

Proof. This follows from Zsigmondy's theorem: each successive quotient $(2^{p^{k+1}} - 1)/(2^{p^k} - 1)$ has a new prime factor. □

Claim (Main claim)**.** Assume n satisfies the problem conditions. Then both the previous claims are sharp in the following sense: each T_i has *exactly* e_i distinct prime divisors, and

$$\left\{ \text{primes dividing } \prod_{i=1}^{m} T_i \right\} = \left\{ \text{primes dividing } 2^n - 1 \right\}.$$

Proof. Rather than try to give a size contradiction directly from here, the idea is to define an ancillary function

$$s(x) = \sum_{p \text{ prime}} \nu_p(x)$$

which computes the sum of the exponents in the prime factorization. For example

$$s(n) = e_1 + e_2 + \dots + e_m.$$

On the other hand, using the earlier claim, we get

$$s(d(2^n - 1)) \ge s\left(d\left(\prod T_i\right)\right) \ge e_1 + e_2 + \dots + e_m = s(n).$$

But we were told that $d(2^n - 1) = n$; hence equality holds in all our estimates, as needed. □

At this point, we may conclude directly that $m = 1$ in any solution; indeed if $m \ge 2$ and $n \ge 7$, Zsigmondy's theorem promises a primitive prime divisor of $2^n - 1$ not dividing any of the T_i.

Now suppose $n = p^e$, and $d(2^{p^e} - 1) = n = p^e$. Since $2^{p^e} - 1$ has exactly e distinct prime divisors, this can only happen if in fact

$$2^{p^e} - 1 = q_1^{p-1} q_2^{p-1} \dots q_e^{p-1}$$

for some distinct primes $q_1, q_2, \dots, q_e$. This is impossible modulo 4 unless $p = 2$.

So we are left with just the case $n = 2^e$, and need to prove $e \le 5$. The proof consists of simply remarking that $2^{2^5} + 1$ is known to not be prime, and hence for $e \ge 6$ the number $2^{2^e} - 1$ always has at least $e + 1$ distinct prime factors.