Problem 2.16

1 Problem Statement

For positive integers a, s, t, prove that:

$$a^{\gcd(s,t)} - 1 = \gcd(a^s - 1, a^t - 1).$$

As a bonus, it can be proven that for any positive integer $n > 1$, $n \nmid 2^n - 1$.

2 Proof of the Main Problem

First, we prove the following lemma:

Lemma 1: For any positive integers a, m, n, if $m \mid n$, then $a^m - 1 \mid a^n - 1$.

Proof of Lemma 1: There exists an integer l such that $m \cdot l = n$. We can then derive the following equation:

$$a^n - 1 = (a^m - 1) \cdot \sum_{i=0}^{l-1} a^{i \cdot m}.$$

Thus, $a^m - 1 \mid a^n - 1$.

Now, let us assume that $s = s_1 \cdot \gcd(s,t)$ and $t = t_1 \cdot \gcd(s,t)$, according to the properties of the greatest common divisor.

We can rewrite the original equation as the intersection of the following two propositions:

$$P : a^{\gcd(s,t)} - 1 \mid \gcd(a^s - 1, a^t - 1),$$
$$Q : \gcd(a^s - 1, a^t - 1) \leq a^{\gcd(s,t)} - 1.$$

For proposition P, we can use Lemma 1 to deduce that $a^{\gcd(s,t)} - 1 \mid a^s - 1$ and $a^{\gcd(s,t)} - 1 \mid a^t - 1$, which implies $a^{\gcd(s,t)} - 1 | \gcd(a^s - 1, a^t - 1)$. Thus, proposition P is true.

For proposition Q, we can use the Bézout's identity to find positive integers k and l such that $k \cdot s - l \cdot t = \gcd(s,t)$. By Lemma 1, we have $a^s - 1 \mid a^{k \cdot s} - 1$ and $a^t - 1 \mid a^{l \cdot t} - 1$. Hence, we obtain:

$$\gcd(a^s - 1, a^t - 1) \mid \gcd(a^{k \cdot s} - 1, a^{l \cdot t} - 1).$$

And since

$$\begin{aligned}
\gcd(a^s - 1, a^t - 1) &\leq \gcd(a^{k \cdot s} - 1, a^{l \cdot t} - 1) \\
&= \gcd((a^{k \cdot s} - 1) - a^{\gcd(s,t)} \cdot (a^{l \cdot t} - 1), a^{l \cdot t} - 1) \\
&= \gcd(a^{\gcd(s,t)} - 1, a^{l \cdot t} - 1) \\
&\leq a^{\gcd(s,t)} - 1.
\end{aligned}$$

So, proposition Q is also true. Thus, we have proven the original equation.

3 Proof of the Bonus

For the case where n is even, we have $2 \mid n$ and $2 \nmid 2^n - 1$, thus we can deduce $n \nmid 2^n - 1$.

For the case where $n \geq 3$ and n is odd, there exists a smallest prime number p that divides n. Since n is odd, p is coprime with 2, and by Fermat's Little Theorem, we have $p \mid 2^{p-1} - 1$.

Now, suppose $n \mid 2^n - 1$, which implies $p \mid 2^n - 1$. Applying the result from the main problem (with $a = 2, s = p - 1, t = n$), we have $p \mid 2^{\gcd(p-1,n)} - 1$. Since p is the smallest prime that divides n, we have $\gcd(p-1, n) = 1$, which leads to $p \mid 1$, a contradiction. Hence, our assumption $n \mid 2^n - 1$ is not true, and we conclude that $n \nmid 2^n - 1$.