Problem 15. Let $a$, $b$, and $n$ be positive integers with $n \geq 2$. Prove that

$$\gcd(n^a - 1, n^b - 1) = n^{\gcd(a, b)} - 1.$$ 

Solution. First note that because $\gcd(a, b)$ is a factor of both $a$ and $b$, it follows that $n^{\gcd(a, b)} - 1$ is a factor of $n^a - 1$ and of $n^b - 1$. Thus $n^{\gcd(a, b)} - 1$ is a factor of $\gcd(n^a - 1, n^b - 1)$.

There are positive integers $x$ and $y$ with $ax - by = \gcd(a, b)$. Now $n^a - 1$ is a factor of $n^{ax} - 1$ and $n^b - 1$ is a factor of $n^{by} - 1$. To connect these, use the equality

$$n^{by}(n^{\gcd(a, b)} - 1) = (n^{ax} - 1) - (n^{by} - 1).$$

Now $\gcd(n^a - 1, n^b - 1)$ divides the right side of this equality, and is relatively prime to $n^{by}$. Thus $\gcd(n^a - 1, n^b - 1)$ is a factor of $n^{\gcd(a, b)} - 1$.

Thus,

$$\gcd(n^a - 1, n^b - 1) = n^{\gcd(a, b)} - 1.$$