LEMMA 0.1. *Let N be a Carmichael number. Then N is not the power of a prime number.*

Proof. Let $N = p^k$ with $p, k \in \mathbb{Z}_{\geq 2}$ and p prime (the case $k = 1$ is trivial). Using the binomial theorem, we have

$$(1 + p^{k-1})^p = \sum_{i=0}^{p} \binom{p}{i} (p^{k-1})^i = 1 + p^k + \binom{p}{2} p^{2k-2} + \dots,$$

that is, $(1 + p^{k-1})^p$ is equal to 1 plus integers that are multiples of $p^k = N$. This implies $(1 + p^{k-1})^p \equiv 1 \mod N$. Hence the order of $1 + p^{k-1}$ in $\mathbb{Z}_N$ is a divisor of p. But since p is prime and clearly $1 + p^{k-1} \neq 1 \mod N$, the order of $1 + p^{k-1}$ is exactly p.

Now suppose that N is Carmichael. Since $gcd(1 + p^{k-1}, N) = 1$, we have that $(1 + p^{k-1})^{N-1} \equiv 1 \mod N$. Since p is the order of $1 + p^{k-1}$ in $\mathbb{Z}_N$, we get that $N - 1$ is a multiple of p, that is, p divides $N - 1$. But this is impossible, since p divides N.