QUESTION

Let $n = q_1 q_2 \dots q_k$ where the q_i are distinct primes and $k > 1$. Show that if n is a Carmichael number then $q_i - 1 | n - 1$ for each i. (This is the converse of the result you proved in example sheet 4, no. 5). Hence show that there is no Carmichael number of the form $3.5.q$, where q is any prime > 5.

ANSWER

Suppose n is a Carmichael number. The, for any b satisfying $\gcd(b, n) = 1$, we have $b^{n-1} \equiv 1 \bmod n$, Now q_i is prime, so we can find a primitive element g_i say mod q_i. The q_i are distinct, so the Chinese Remainder Theorem allows us to find a unique solution mod n to the simultaneous congruences $x \equiv g_i$ mod q_i for $1 \leq i \leq n$. Let b be this unique solution. The $\gcd(b, n) = 1$ since $\gcd(b, q_i) = 1$ for each i. Thus $b^{n-1} \equiv 1 \bmod n$, and so $b^{n-1} \equiv 1 \bmod q_i$ for each i. But $b \equiv g_i \bmod q_i$, and g_i has order $q_i - 1 \bmod q_i$ as g_i is a primitive element mod q_i. Thus $q_i - 1 | n - 1$, and this is true for each i, as required.
Now suppose $n = 3.5.q$ is a Carmichael number, where q is a prime > 5, By the above, n is divisible by 2,4 and $q - 1$. Set $q - 1 = t$. Then $n = 15(t + 1)$, so $n - 1 = 15t + 14$. Since $t | n - 1$ we have $t | 14$. Thus t=1,2,7 or 14, which makes $q = t + 1$ equal to 2,3,8 or 25, none of which is a prime > 5. Thus no such Carmichael number exists.