QUESTION

Let $n = q_1q_2 \dots q_k$, where the q_i are distinct primes and $k > 1$. Suppose that for each i, $q_i - 1|n - 1$. Show that n is a Carmichael number.

Hence find a Carmichael number of the form $7.23.q$ where q is an odd prime.

ANSWER

$n = q_1q_2 \dots q_k$, q_i distinct primes, and $k > 1$. Thus, as $k > 1$, n is composite. Suppose $\gcd(b, n) = 1$. Thus $\gcd b, q_i) = 1$ for each i. Hence $b^{p_i-1} \equiv 1 \bmod q_i$ by Fermat's Little Theorem. But $q_i - 1|n - 1$, say $(q_i - 1)s = (n - 1)$ for some s. Thus $b^{n-1} = (b^{q_i-1})^s \equiv 1^1 \equiv 1 \bmod q_i$. Thus $q_i|b^{n-1} - 1$, and this is true for each i, so we get $q_1q_1 \dots q_k|b^{n-1} - 1$ by cor.1.7. But$n = q_1q_2 \dots q_k$, so $n|b^{n-1} - 1$ and $b^{n-1} \equiv 1 \bmod n$. Thus n is a Carmichael number as required.

Suppose q is an odd prime $\neq 7, 23$. By the above proof, $n = 7.23.q$ will be a Carmichael number if each of 6,22,$q - 1$ divides $n - 1$.

Consider the equation $n = 7.23.q$ modulo 6. Since $6|n - 1$, we have $n \equiv 1 \bmod 6$, and so $\equiv 1. - 1.q \bmod 6$, giving $q \equiv -1 \bmod 6$. Similarly, reducing the equation $n = 7.23.q \bmod 22$, we get $1 \equiv 7.1.q \bmod 22$, or, on multiplying by 3, $3 \equiv -1.q \bmod 22$. Thus $q \equiv -3 \bmod 22$. Finally, reducing the equation $n = 7.23.q \bmod (q-1)$, we get $1 \equiv 7.23.1 \bmod q-1$, ei.e. $160 \equiv 0 \bmod (q-1)$, so that $q - 1$ divides 160. To find a prime satisfying all three requirements, we may start listing positive integers congruent to $-3 \bmod 22$, checking each in turn to see of they satisfy the other two requirements, $q \equiv -1 \bmod 6$, and $q-1$ divides 160. Our process either produces a positive integer satisfying our requirements, or leads to numbers larger than 160, so that we could conclude that no such integer q existed. In any case the process will terminate. We check $q = 19$m which fails, then $q = 41$, which is prime and satisfies all our conditions, so 7.23.41 is a suitable Carmichael number.