(b) *If n is square free, then n is a Carmichael number if and only if $p-1|n-1$ for every prime p dividing n.*

Proof. (a) Suppose that $p^2|n$. Let g be a generator modulo p^2, i.e., an integer such that $g^{p(p-1)}$ is the lowest power of g which is $\equiv 1$ *mod* p^2. According to Exercise 2 of § II.1, such a g always exists. Let n' be the product of all primes other than p which divide n. By the Chinese Remainder Theorem, there is an integer b satisfying the two congruences: $b \equiv g$ *mod* p^2 and $b \equiv 1$ *mod* n'. Then b is, like g, a generator modulo p^2, and it also satisfies $g.c.d.(b, n) = 1$, since it is not divisible by p or by any prime which divides n'. We claim that n is not a pseudoprime to the base b. To see this, we notice that if (1) holds, then, since $p^2|n$, we automatically have $b^{n-1} \equiv 1$ *mod* p^2. But in that case $p(p-1)|n-1$, since $p(p-1)$ is the order of b modulo p^2. However, $n-1 \equiv -1$ *mod* p, since $p|n$, and this means that $n-1$ is not divisible by $p(p-1)$. This contradiction proves that there is a base b for which n fails to be a pseudoprime.

(b) First suppose that $p-1|n-1$ for every p dividing n. Let b be any base, where $g.c.d.(b, n) = 1$. Then for every prime p dividing n we have: b^{n-1} is a power of b^{p-1}, and so is $\equiv 1$ *mod* p. Thus, $b^{n-1}-1$ is divisible by all of the prime factors p of n, and hence by their product, which is n. Hence, (1) holds for all bases b. Conversely, suppose that there is a p such that $p-1$ does not divide $n-1$. Let g be an integer which generates $(\mathbf{Z}/p\mathbf{Z})^*$. As in the proof of part (a), find an integer b which satisfies: $b \equiv g$ *mod* p and $b \equiv 1$ *mod* n/p. Then $g.c.d.(b, n) = 1$, and $b^{n-1} \equiv g^{n-1}$ *mod* p. But g^{n-1} is not $\equiv 1$ *mod* p, because $n-1$ is not divisible by the order $p-1$ of g. Hence, $b^{n-1} \not\equiv 1$ *mod* p, and so (1) cannot hold. This completes the proof of the proposition.

Example 2. $n = 561 = 3 \cdot 11 \cdot 17$ is a Carmichael number, since 560 is divisible by $3-1$, $11-1$ and $17-1$. In the exercises we shall see that this is the smallest Carmichael number.

Proposition V.1.3. *A Carmichael number must be the product of at least three distinct primes.*

Proof. By Proposition V.1.2, we know that a Carmichael number must be a product of distinct primes. So it remains to rule out the possibility that $n = pq$ is the product of two distinct primes. Suppose that $p < q$. Then, if n were a Carmichael number, we would have $n-1 \equiv 0$ *mod* $q-1$, by part (b) of Proposition V.1.2. But $n-1 = p(q-1+1)-1 \equiv p-1$ *mod* $q-1$, and this is not $\equiv 0$ *mod* $q-1$, since $0 < p-1 < q-1$. This concludes the proof.

Remark. It was only very recently that it was proved (by Alford, Granville, and Pomerance) that there exist infinitely many Carmichael numbers. See Granville's report in *Notices of the Amer. Math. Soc.* **39** (1992), 696–700.

Euler pseudoprimes. Let n be an odd integer, and let $\left(\frac{b}{n}\right)$ denote the Jacobi symbol (see § II.2). According to Proposition II.2.2, if n is a prime number, then