(b) *If n is a pseudoprime to the bases b_1 and b_2 (where $g.c.d.(b_1, n) = = g.c.d.(b_2, n) = 1$), then n is a pseudoprime to the base b_1b_2 and also to the base $b_1b_2^{-1}$ (where b_2^{-1} is an integer which is inverse to b_2 modulo n).*

(c) *If n fails the test (1) for a single base $b \in (\mathbf{Z}/n\mathbf{Z})^*$, then n fails (1) for at least half of the possible bases $b \in (\mathbf{Z}/n\mathbf{Z})^*$.*

Proof. Parts (a) and (b) are very easy, and will be left to the reader. To prove (c), let $\{b_1, b_2, \ldots, b_s\}$ be the set of all bases for which n is a pseudoprime, i.e., the set of all integers $0 < b_i < n$ for which the congruence (1) holds. Let b be a fixed base for which n is not a pseudoprime. If n were a pseudoprime for any of the bases bb_i, then, by part (b), it would be a pseudoprime for the base $b \equiv (bb_i)b_i^{-1}$ *mod* n, which is not the case. Thus, for the s distinct residues $\{bb_1, bb_2, \ldots, bb_s\}$ the integer n fails the test (1). Hence, there are at least as many bases in $(\mathbf{Z}/n\mathbf{Z})^*$ for which n fails to be a pseudoprime as there are bases for which (1) holds. This completes the proof.

Thus, unless n happens to pass the test (1) for *all* possible b with $g.c.d.(b, n) = 1$, we have at least a 50% chance that n will fail (1) for a randomly chosen b. That is, suppose we want to know if a large odd integer n is prime. We might choose a random b in the range $0 < b < n$. We first find $d = g.c.d.(b, n)$ using the Euclidean algorithm. If $d > 1$, we know that n is not prime, and in fact we have found a nontrivial factor $d|n$. If $d = 1$, then we raise b to the $(n-1)$-st power (using the repeated squaring method of modular exponentiation, see § I.3). If (1) fails, we know that n is composite. If (1) holds, we have some evidence that perhaps n is prime. We then try another b and go through the same process. If (1) fails for any b, then we can stop, secure in the knowledge that n is composite. Suppose that we try k different b's and find that n is a pseudoprime for all of the k bases. By Proposition V.1.1, the chance that n is still composite despite passing the k tests is at most 1 out of 2^k, *unless* n happens to have the very special property that (1) holds for every single $b \in (\mathbf{Z}/n\mathbf{Z})^*$. If k is large, we can be sure "with a high probability" that n is prime (unless n has the property of being a pseudoprime for all bases). This method of finding prime numbers is called a *probabilistic* method. It differs from a *deterministic* method: the word "deterministic" means that the method will either reveal n to be composite or else determine with 100% certainty that n is prime.

Can it ever happen for a composite n that (1) holds for every b? In that case our probabilistic method fails to reveal the fact that n is composite (unless we are lucky and hit upon a b with $g.c.d.(b, n) > 1$). The answer is yes, and such a number is called a *Carmichael number.*

Definition. A *Carmichael number* is a composite integer n such that (1) holds for every $b \in (\mathbf{Z}/n\mathbf{Z})^*$.

Proposition V.1.2. *Let n be an odd composite integer.*

(a) *If n is divisible by a perfect square > 1, then n is not a Carmichael number.*