$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \mathit{mod}\ n \tag{2}$$

for any integer b. On the other hand, if n is composite, then Exercise 21 of § II.2 shows that at least 50% of all $b \in (\mathbf{Z}/n\mathbf{Z})^*$ fail to satisfy (2). From these two facts we can obtain an efficient probabilistic test for whether or not a large odd integer n is prime. We start with the following definition.

Definition. If n is an odd composite number and b is an integer such that $g.c.d.(n, b) = 1$ and (2) holds, then n is called an *Euler pseudoprime to the base b*.

Proposition V.1.4. *If n is an Euler pseudoprime to the base b, then it is a pseudoprime to the base b.*

Proof. We must show that, if (2) holds, then (1) holds. But this is obvious by squaring both sides of the congruence (2).

Example 3. The converse of Proposition V.1.4 is false. For example, in Example 1 we saw that 91 is a pseudoprime to the base 3. However, $3^{45} \equiv 27\ \mathit{mod}\ 91$, so (2) does not hold for $n = 91$, $b = 3$. (Note that it is easy to raise b to a large power modulo 91 if we know the order of b in $(\mathbf{Z}/91\mathbf{Z})^*$; since $3^6 \equiv 1\ \mathit{mod}\ 91$, we immediately see that $3^{45} \equiv 3^3\ \mathit{mod}\ 91$.) An example of a base to which 91 is an Euler pseudoprime is 10, since $10^{45} \equiv 10^3 \equiv -1\ \mathit{mod}\ 91$, and $(\frac{10}{91}) = -1$.

Example 4. It is easy to see that any odd composite n is an Euler pseudoprime to the base ± 1; in what follows we shall rule out these two "trivial" bases b.

We can now describe the **Solovay–Strassen primality test**. Suppose that n is a positive odd integer, and we would like to know whether n is prime or composite. Choose k integers $0 < b < n$ at random. For each b, first compute both sides of (2). Finding the left side $b^{(n-1)/2}$ takes $O(log^3 n)$ bit operations, using the repeated squaring method (Proposition I.3.6); finding the Jacobi symbol on the right also takes $O(log^3 n)$ bit operations (see Exercise 17 of § II.2). If the two sides are not congruent modulo n, then you know that n is composite, and the test stops. Otherwise, move on to the next b. If (2) holds for all k random choices of b, then the probability that n is composite despite passing all of the tests is at most $1/2^k$. Thus, the Solovay–Strassen test is a probabilistic algorithm which leads either to the conclusion that n is composite or to the conclusion that it is "probably" prime.

Notice that there are no Euler pseudoprime analogs of Carmichael numbers: for *any* composite n, the test (2) fails for at least half of the possible bases b.

Strong pseudoprimes. We now discuss one more type of primality test, which is in one respect even better than the Solovay–Strassen test based on the definition of an Euler pseudoprime. This is the Miller–Rabin test, which is based on the notion of a "strong pseudoprime," which will be defined below. Suppose that n is a large positive odd integer, and $b \in (\mathbf{Z}/n\mathbf{Z})^*$. Suppose that n is a pseudoprime to the base b, i.e., $b^{n-1} \equiv 1\ \mathit{mod}\ n$.