The idea behind the strong pseudoprime criterion is that, if we successively "extract square roots" of this congruence, i.e., if we raise b to the $((n-1)/2)$-th, $((n-1)/4)$-th, ..., $((n-1)/2^s)$-th powers (where $t = (n-1)/2^s$ is odd), then the first residue class we get other than 1 must be -1 if n is prime, because ± 1 are the only square roots of 1 modulo a prime number. Actually, in practice one proceeds in the other direction, setting $n - 1 = 2^s t$ with t odd, then computing b^t *mod* n, then (if that is not $\equiv 1$ *mod* n) squaring to get b^{2t} *mod* n, then squaring again to get $b^{2^2 t}$ *mod* n, etc., until we first obtain the residue 1; then the step before getting 1 we must have had -1, or else we know that n is composite.

Definition. Let n be an odd composite number, and write $n - 1 = 2^s t$ with t odd. Let $b \in (\mathbf{Z}/n\mathbf{Z})^*$. If n and b satisfy the condition

$$\text{either } b^t \equiv 1 \ mod\ n \quad \text{or} \quad \text{there exists } r,\ 0 \le r < s, \text{ such that } b^{2^r t} \equiv -1 \ mod\ n, \tag{3}$$

then n is called a *strong pseudoprime to the base b*.

Proposition V.1.5. *If* $n \equiv 3$ *mod* 4, *then* n *is a strong pseudoprime to the base* b *if and only if it is an Euler pseudoprime to the base* b.

Proof. Since in this case $s = 1$ and $t = (n-1)/2$, we see that n is a strong pseudoprime to the base b if and only if $b^{(n-1)/2} \equiv \pm 1$ *mod* n. If n is an Euler pseudoprime, then this congruence holds, by definition. Conversely, suppose that $b^{(n-1)/2} \equiv \pm 1$. We must show that the ± 1 on the right is $(\frac{b}{n})$. But for $n \equiv 3$ *mod* 4 we have $\pm 1 = (\frac{\pm 1}{n})$, and so

$$\left(\frac{b}{n}\right) = \left(\frac{b \cdot (b^2)^{(n-3)/4}}{n}\right) = \left(\frac{b^{(n-1)/2}}{n}\right) \equiv b^{(n-1)/2} \ mod\ n,$$

as required. The next two important propositions are somewhat harder to prove.

Proposition V.1.6. *If* n *is a strong pseudoprime to the base* b, *then it is an Euler pseudoprime to the base* b.

Proposition V.1.7. *If* n *is an odd composite integer, then* n *is a strong pseudoprime to the base* b *for at most 25% of all* $0 < b < n$.

Remark. The converse of Proposition V.1.6 is not true, in general, as we shall see in the exercises below.

Before proving these two propositions, we describe the **Miller–Rabin primality test**. Suppose we want to determine whether a large positive odd integer n is prime or composite. We write $n-1 = 2^s t$ with t odd, and choose a random integer b, $0 < b < n$. First we compute b^t *mod* n. If we get ± 1, we conclude that n passes the test (3) for our particular b, and we go on to another random choice of b. Otherwise, we square b^t modulo n, then square that modulo n, and so on, until we get -1. If we get -1, then n passes the test. However, if we never obtain -1, i.e., if we reach $b^{2^{r+1}} \equiv 1$ *mod* n while $b^{2^r} \not\equiv -1$ *mod* n, then n fails the test and we know that n is composite. If n passes the test (3) for all our random choices of b — suppose we try k different bases b — then we know by Proposition V.1.7 that n has at most a