1 out of 4^k chance of being composite. This is because, if n is composite, then at most $1/4$ of the bases $0 < b < n$ satisfy (3). Notice that this is somewhat better than for the Solovay–Strassen test, where the analogous estimate is a 1 out of 2^k chance (because there exist composite n which are Euler pseudoprimes for half of all bases $0 < b < n$, as we shall see in the exercises).

We now proceed to the proofs of Propositions V.1.6 and V.1.7.

Proof of Proposition V.1.6. We have n and b satisfying (3). We must prove that they satisfy (2). Let $n-1 = 2^s t$ with t odd.

Case (i). First suppose that $b^t \equiv 1 \ mod\ n$. Then the left side of (2) is clearly 1. We must show that $(\frac{b}{n}) = 1$. But $1 = (\frac{1}{n}) = (\frac{b^t}{n}) = (\frac{b}{n})^t$. Since t is odd, this means that $(\frac{b}{n}) = 1$.

Case (ii). Next suppose that $b^{(n-1)/2} \equiv -1 \ mod\ n$. Then we must show that $(\frac{b}{n}) = -1$. Let p be any of the prime divisors of n. We write $p-1$ in the form $p - 1 = 2^{s'} t'$ with t' odd, and we prove the following claim:

Claim. *We have $s' \geq s$, and*

$$\left(\frac{b}{p}\right) = \begin{cases} -1, & \text{if } s' = s; \\ 1, & \text{if } s' > s. \end{cases}$$

Proof of the claim. Because $b^{(n-1)/2} = b^{2^{s-1}t} \equiv -1 \ mod\ n$, raising both sides to the t' power gives $(b^{2^{s-1}t'})^t \equiv -1 \ mod\ n$. Since $p|n$, the same congruence holds modulo p. But if we had $s' < s$, this would mean that $b^{2^{s'}t'}$ could not be $\equiv 1 \ mod\ p$, as it must be by Fermat's Little Theorem. Thus, $s' \geq s$. If $s' = s$, then the congruence $(b^{2^{s-1}t'})^t \equiv -1 \ mod\ p$ implies that $(\frac{b}{p}) \equiv b^{(p-1)/2} = b^{2^{s'-1}t'} \ mod\ p$ must be -1 rather than 1. On the other hand, if $s' > s$, then the same congruence raised to the $(2^{s'-s})$-th power implies that $(\frac{b}{p})$ must be 1 rather than -1. This proves the claim.

We now return to the proof of Proposition V.1.6 in Case (ii). We write n as a product of primes (*not* necessarily distinct): $n = \prod p$. Let k denote the number of primes p such that $s' = s$ when one writes $p - 1 = 2^{s'}t'$ with t' odd. (k counts such a prime p with its multiplicity, i.e., α times if $p^\alpha || n$.) According to the claim, we always have $s' \geq s$, and $(\frac{b}{n}) = \prod (\frac{b}{p}) = (-1)^k$. On the other hand, working modulo 2^{s+1}, we see that $p \equiv 1$ unless p is one of the k primes for which $s' = s$, in which case $p \equiv 1 + 2^s$. Since $n = 1 + 2^s t \equiv 1 + 2^s \ mod\ 2^{s+1}$, we have $1 + 2^s \equiv \prod p \equiv (1+2^s)^k \equiv 1 + k2^s \ mod\ 2^{s+1}$ (where the last step follows by the binomial expansion). This means that k must be odd, and hence $(\frac{b}{n}) = (-1)^k = -1$, as was to be proved.

Case (iii). Finally, suppose that $b^{2^{r-1}t} \equiv -1 \ mod\ n$ for some $0 < r < s$. (We are using $r - 1$ in place of the r in (3).) Since then $b^{(n-1)/2} \equiv 1 \ mod\ n$, we must show that in Case (iii) we have $(\frac{b}{n}) = 1$. Again let p be any prime divisor of n, and write $p - 1 = 2^{s'}t'$ with t' odd.

Claim. *We have $s' \geq r$, and*

$$\left(\frac{b}{p}\right) = \begin{cases} -1, & \text{if } s' = r; \\ 1, & \text{if } s' > r. \end{cases}$$