$$\frac{p-1}{p^2-1} = \frac{1}{p+1} \leq \frac{1}{4}.$$

Since the proportion of b in the range from 0 to n which satisfy $b^{n-1} \equiv 1 \ mod\ n$ is less than or equal to this, we conclude that n is a pseudoprime to the base b for at most 1/4 of the b, $0 < b < n$. This proves the proposition in Case (i). (**Remark:** This upper bound of 25% is actually reached in Case (i) in the case when $n = 9$, i.e., 9 is a (strong) pseudoprime for 2 out of the 8 possible values of b, namely, $b = \pm 1$.)

Case (ii). We next suppose that n is the product of 2 distinct primes p and q: $n = pq$. We write $p - 1 = 2^{s'}t'$ with t' odd and $q - 1 = 2^{s''}t''$ with t'' odd. Without loss of generality we may suppose that $s' \leq s''$. In order for an element $b \in (\mathbf{Z}/n\mathbf{Z})^*$ to be a base to which n is a strong pseudoprime, one of the following must occur: (1) $b^t \equiv 1 \ mod\ p$ and $b^t \equiv 1 \ mod\ q$, or (2) $b^{2^r t} \equiv -1 \ mod\ p$ and $b^{2^r t} \equiv -1 \ mod\ q$ for some r, $0 \leq r < s$. According to Lemma 1, the number of b for which the first possibility holds is the product of $g.c.d.(t, t')$ (the number of residue classes modulo p) times $g.c.d.(t, t'')$ (the number of residue classes modulo q), which is certainly no greater than $t't''$. According to Lemma 2, for each $r < \min(s', s'') = s'$ the number of b for which $b^{2^r t} \equiv -1 \ mod\ n$ is $2^r g.c.d.(t, t') \cdot 2^r g.c.d.(t, t'') < 4^r t't''$. Since we have $n - 1 > \varphi(n) = 2^{s'+s''}t't''$, it follows that the fraction of integers b, $0 < b < n$, for which n is a strong pseudoprime is at most

$$\frac{t't'' + t't'' + 4t't'' + 4^2 t't'' + \cdots + 4^{s'-1}t't''}{2^{s'+s''}t't''} = 2^{-s'-s''}\left(1 + \frac{4^{s'} - 1}{4 - 1}\right).$$

If $s'' > s'$, then this is at most $2^{-2s'-1}(\frac{2}{3} + \frac{4^{s'}}{3}) \leq 2^{-3}\frac{2}{3} + \frac{1}{6} = \frac{1}{4}$, as desired. On the other hand, if $s' = s''$, then we note that one of the two inequalities $g.c.d.(t, t') \leq t'$, $g.c.d.(t, t'') \leq t''$ must be a strict inequality, since if we had $t'|t$ and $t''|t$, we could conclude from the congruence $n - 1 = 2^s t = pq - 1 \equiv q - 1 \ mod\ t'$ that $t'|q - 1 = 2^{s''}t''$, i.e., $t'|t''$, and similarly $t''|t'$; but this would mean that $t' = t''$ and $p = q$, a contradiction. Hence one of the two g.c.d.'s is strictly less than t' or t'', and so must be less at least by a factor of 3 (since we're working with odd numbers). Thus, in this case we may replace $t't''$ by $\frac{1}{3}t't''$ in the above estimates for the number of b satisfying each condition for n to be a strong pseudoprime to the base b. This leads to the following upper bound for the fraction of integers b, $0 < b < n$, for which n is a strong pseudoprime:

$$\frac{1}{3}2^{-2s'}\left(\frac{2}{3} + \frac{4^{s'}}{3}\right) \leq \frac{1}{18} + \frac{1}{9} = \frac{1}{6} < \frac{1}{4},$$

as desired. This completes the proof of the theorem in Case (ii).

Case (iii). Finally, we suppose that n is a product of more than 2 distinct primes: $n = p_1 p_2 \cdots p_k$, $k \geq 3$. We write $p_j - 1 = 2^{s_j}t_j$ with t_j odd, and we proceed exactly as in Case (ii). Without loss of generality, we may