The proof of this claim is identical to the proof of the claim in Case (ii).

To prove the proposition in Case (iii), we let k denote the number of primes p (not necessarily distinct) in the product $n = \prod p$ for which the first alternative holds, i.e., $s' = r$. Then, as in Case (ii), we obviously have $(\frac{b}{n}) = (-1)^k$. On the other hand, since $n = 1 + 2^s t \equiv 1 \bmod 2^{r+1}$ and also $n = \prod p \equiv (1+2^r)^k \bmod 2^{r+1}$, it follows that k must be even, i.e., $(\frac{b}{n}) = 1$. This concludes the proof of Proposition V.1.6.

Before proving Proposition V.1.7, we prove a general lemma about the number of solutions to the equation $x^k = 1$ in a "cyclic group" containing m elements. We already encountered this lemma once at the beginning of § II.2; the proof of the lemma should be compared to the proof of Proposition II.2.1.

Lemma 1. *Let $d = g.c.d.(k, m)$. Then there are exactly d elements in the group $\{g, g^2, g^3, \ldots, g^m = 1\}$ which satisfy $x^k = 1$.*

Proof. An element g^j satisfies the equation if and only if $g^{jk} = 1$, i.e., if and only if $m|jk$. This is equivalent to: $\frac{m}{d}|j\frac{k}{d}$, which, since m/d and k/d are relatively prime, is equivalent to: j is a multiple of m/d. There are d such values of j, $1 \le j \le m$. This proves the lemma.

We need one more lemma, which has a proof similar to that of Lemma 1.

Lemma 2. *Let p be an odd prime, and write $p - 1 = 2^{s'}t'$ with t' odd. Then the number of $x \in (\mathbf{Z}/p\mathbf{Z})^*$ which satisfy $x^{2^r t} \equiv -1 \bmod p$ (where t is odd) is equal to 0 if $r \ge s'$ and is equal to $2^r g.c.d.(t, t')$ if $r < s'$.*

Proof. We let g be a generator of $(\mathbf{Z}/p\mathbf{Z})^*$, and we write x in the form g^j with $0 \le j < p - 1$. Since $g^{(p-1)/2} \equiv -1 \bmod p$ and $p - 1 = 2^{s'}t'$, the congruence in the lemma is equivalent to: $2^r tj \equiv 2^{s'-1}t' \bmod 2^{s'}t'$ (with j the unknown). Clearly there is no solution if $r > s' - 1$. Otherwise, we divide out by the g.c.d. of the modulus and the coefficient of the unknown, which is $2^r d$, where $d = g.c.d.(t, t')$. The resulting congruence has a unique solution modulo $2^{s'-r}\frac{t'}{d}$, and it has $2^r d$ solutions modulo $2^{s'}t'$, as claimed. This proves Lemma 2.

Proof of Proposition V.1.7. Case (i). We first suppose that n is divisible by the square of some prime p. Say $p^\alpha || n$, $\alpha \ge 2$. We show that in this case n cannot even be a pseudoprime (let alone a strong pseudoprime) for more than $(n-1)/4$ bases b, $0 < b < n$. To do this, we suppose that $b^{n-1} \equiv 1 \bmod n$, which implies that $b^{n-1} \equiv 1 \bmod p^2$, and we find a condition modulo p^2 that b must satisfy. Recall that $(\mathbf{Z}/p^2\mathbf{Z})^*$ is a cyclic group of order $p(p-1)$ (see Exercise 2 of § II.1), i.e., there exists an integer g such that $(\mathbf{Z}/p^2\mathbf{Z})^* = \{g, g^2, g^3, \ldots, g^{p(p-1)}\}$. According to Lemma 1, the number of possibilities for b modulo p^2 for which $b^{n-1} \equiv 1 \bmod p^2$ is $d = g.c.d.(p(p-1), n-1)$. Since $p|n$, it follows that $p \nmid n - 1$, and hence $p \nmid d$. Thus, the largest d can be is $p - 1$. Hence, the proportion of all b not divisible by p^2 in the range from 0 to n which satisfy $b^{n-1} \equiv 1 \bmod p^2$ is less than or equal to