suppose that $s_1 \leq s_j$ is the smallest of the s_j. We obtain the following upper bound for the fraction of possible b's for which n is a strong pseudoprime:

$$2^{-s_1-s_2-\cdots-s_k}\left(1+\frac{2^{ks_1}-1}{2^k-1}\right) \leq 2^{-ks_1}\left(\frac{2^k-2}{2^k-1}+\frac{2^{ks_1}}{2^k-1}\right) =$$

$$= 2^{-ks_1}\frac{2^k-2}{2^k-1}+\frac{1}{2^k-1} \leq 2^{-k}\frac{2^k-2}{2^k-1}+\frac{1}{2^k-1} = 2^{1-k} \leq \frac{1}{4},$$

because $k \geq 3$ in Case (iii). This concludes the proof of Proposition V.1.7.

Remarks. **1.** In fact, in practice one does not have to choose a very large number of bases b to be almost sure that n is prime if it is a strong pseudoprime to each base b. For example, it has been computed that there is only one composite number less than $2.5 \cdot 10^{10}$ — namely, $n = 3215031751$ — which is a strong pseudoprime to all four bases 2, 3, 5, 7.

2. It is not entirely satisfactory to rely upon a probabilistic test. Despite Émile Borel's assurance, quoted at the beginning of the section, it would be nice to have rapid methods to *prove* that a given n really is prime (especially, if it is of some special practical or theoretical importance to know that the particular n is prime). For example, suppose we knew that there is some fairly small B (depending on the size of n) such that, if n is composite, then there is some base $b < B$ for which n is not a strong pseudoprime. If we knew that, then in order to be absolutely sure that n is prime it would suffice to test (3) only for the first B bases.

There is such a fact, but it depends upon an unproved conjecture called the "Generalized Riemann Hypothesis." The usual Riemann Hypothesis is the assertion that all complex zeros of the so-called "Riemann zeta-function" $\zeta(s)$ (which is defined to be the sum of the reciprocal s-th powers when $s > 1$) which lie in the "critical strip" (where the real part of s is between 0 and 1) must lie on the "critical line" (where the real part of s is 1/2). The Generalized Riemann Hypothesis is the same assertion for certain generalizations of $\zeta(s)$ called "Dirichlet L-series." The following fact, whose proof is beyond the scope of this book, shows that the Miller–Rabin test (3) gives a *deterministic* primality test which takes polynomial time (in $\log n$), provided that one is willing to assume the validity of the Generalized Riemann Hypothesis (GRH).

If the GRH is true, and if n is a composite odd integer, then n fails the test (3) for at least one base b less than $2\log^2 n$.

3. In the 1980's an efficient deterministic primality test was developed which, while strictly speaking not polynomial in $\log n$, in practice can routinely prove primality of numbers of over a hundred decimal digits in a matter of seconds (on current large computers). This method of Adleman–Pomerance–Rumely and Cohen–Lenstra is based on the same ideas as the primality tests considered above, except that it uses analogs of Fermat's Little Theorem in extension fields of the rational numbers. A basic role is played by Gauss sums (certain types of which were introduced in §II.2 in order to prove quadratic reciprocity) and the closely related "Jacobi