Exercise 1. Suppose that $n = p^e$ is a prime power, and we are given $a$ with $(a, p) = 1$. Show that Miller’s primality test for the base $a$ is no more effective than simply evaluating whether or not $a^{n-1} \equiv 1 \pmod{n}$ (in the book’s terminology, this is saying that if $n$ is a pseudoprime for the base $a$, then in fact $n$ is a strong pseudoprime for the base $a$).

Exercise 2. Do Exercise 2 of Section 4.6 of the textbook.

Exercise 3. Do Exercise 26 of Section 6.1 of the textbook.

Exercise 4. Let $n$ be an odd composite integer, and let $c$ be a multiple of $\phi(n)$. We show that a random choice of base $a$ has a reasonably high chance of factoring $n$ using Miller’s factorization algorithm.

Suppose that $p, q$ are primes dividing $n$. Write $p - 1 = 2^i \cdot s$ and $q - 1 = 2^j \cdot t$, with $s, t$ odd, and suppose without loss of generality that $i \leq j$. Show that if $a$ is any integer with $(a, n) = 1$ such that $a$ is a perfect square modulo $p$ but is not a perfect square modulo $q$, then Miller factorization algorithm will find a nontrivial factor of $n$ when the base $a$ is used.

Exercise 5. Do Exercise 4 of Section 3.6 of the textbook.