(b) Assuming the Generalized Riemann Hypothesis, estimate the number of bit operations required to perform the Miller–Rabin test on n enough times to be sure that, if n passes all the tests, then it is prime.

19. (a) Prove that, if n is a pseudoprime to the base 2, then $N = 2^n - 1$ is a strong pseudoprime and an Euler pseudoprime to the base 2.
(b) Prove that there are infinitely many strong pseudoprimes and Euler pseudoprimes to the base 2.
20. Prove that, if n is a strong pseudoprime to the base b, then it is a strong pseudoprime to the base b^k for any integer k.
21. Let n be the Carmichael number 561.
(a) Find the number of bases $b \in (\mathbf{Z}/561\mathbf{Z})^*$ for which 561 is an Euler pseudoprime.
(b) Find the number of bases for which 561 is a strong pseudoprime, and make a list of them.
22. Prove that if n is a prime power p^α, where $\alpha > 1$, then n is a strong pseudoprime to the base b if and only if it is a pseudoprime to the base b.
23. (a) Show that 65 is a strong pseudoprime to the base 8 and to the base 18, but not to the base 14, which is the product of 8 and 18 modulo 65.
(b) For any odd composite integer n, let $(*)$ denote the assertion, "Whenever n is a strong pseudoprime to the base b_1 and to the base b_2 it is a strong pseudoprime to the base $b = b_1 b_2$" (in other words, the strong pseudoprime property is preserved under multiplication of bases). Prove that $(*)$ holds if and only if n is a prime power or is divisible by a prime which is $\equiv 3 \bmod 4$.
24. (a) Prove that, if you find a b such that n is a pseudoprime but *not* a strong pseudoprime to the base b, then you can quickly find a nontrivial factor of n.
(b) Explain how to guard against this when choosing your $n = pq$ in the RSA cryptosystem.

Remark. In many primality tests, if a composite n happens to pass some initial test and then fails a subsequent test, one not only learns that n is composite, but at the same time one can quickly find a nontrivial factor. Exercise 24 is an example of this: if n passes the pseudoprime test to the base b and then fails the strong pseudoprime test to the base b, then you can factor n. One can easily be misled into thinking that in this way the primality tests can also be used for factorization. This is not the case. Given a large composite number n (e.g., a product of two randomly selected large primes), it is extremely unlikely that we would stumble upon a base b for which n is a pseudoprime (see Exercise 5(a) above to get an idea of the probability of stumbling upon such a b). Thus, the various refined pseudoprime tests are useful only in convincing ourselves of the primality of a number that really is prime; in practice, if we have a composite number