sums." A detailed discussion of their method would take us too far afield. A thorough and readable account is given in the Cohen–Lenstra article in *Mathematics of Computation.*

Exercises

1. (a) Find all bases b for which 15 is a pseudoprime. (Do not include the trivial bases ± 1.)
   (b) Find all bases for which 21 is a pseudoprime.
   (c) Prove that there are 36 bases $b \in (\mathbf{Z}/91\mathbf{Z})^*$ (i.e., 50% of the possible bases) for which 91 is a pseudoprime.
   (d) Generalizing part (c), show that if p and $2p-1$ are both prime, and $n = p(2p-1)$, then n is a pseudoprime for 50% of the possible bases b, namely for all b which are quadratic residues modulo $2p-1$.
2. Let n be a positive odd composite integer, and let $g.c.d.(b,n) = 1$.
   (a) Show that if p is a prime divisor of n and we set set $n' = n/p$, then n is a pseudoprime to the base b only if $b^{n'-1} \equiv 1 \ mod\ p$.
   (b) Prove that no integer of the form $n = 3p$ (with $p > 3$ prime) can be a pseudoprime to the base 2, 5 or 7.
   (c) Prove that no integer of the form $n = 5p$ (with $p > 5$ prime) can be a pseudoprime to the base 2, 3 or 7.
   (d) Prove that 91 is the smallest pseudoprime to the base 3.
3. Show that p^2 (with p prime) is a pseudoprime to the base b if and only if $b^{p-1} \equiv 1 \ mod\ p^2$.
4. (a) Find the smallest pseudoprime to the base 5.
   (b) Find the smallest pseudoprime to the base 2.
5. Let $n = pq$ be a product of two distinct primes.
   (a) Set $d = g.c.d.(p-1, q-1)$. Prove that n is a pseudoprime to the base b if and only if $b^d \equiv 1 \ mod\ n$. In terms of d, how many bases are there to which n is a pseudoprime?
   (b) How many bases are there to which n is a pseudoprime if $q = 2p+1$? List all of them (in terms of p).
   (c) For $n = 341$, what is the probability that a randomly chosen b prime to n will be a base to which n is a pseudoprime?
6. Show that, if n is a pseudoprime to the base $b \in (\mathbf{Z}/n\mathbf{Z})^*$, then n is also a pseudoprime to the base $-b$ and to the base b^{-1}.
7. (a) Prove that if n is a pseudoprime to the base 2, then so is $N = 2^n - 1$.
   (b) Prove that if n is a pseudoprime to the base b, and if $g.c.d.(b-1, n) = 1$, then the integer $N = (b^n - 1)/(b-1)$ is a pseudoprime to the base b.
   (c) Prove that there are infinitely many pseudoprimes to the base b for $b = 2$, 3, 5.
   (d) Give an example showing that part (b) may be false if we omit the condition $g.c.d.(b-1, n) = 1$.