and C. Pomerance have reduced the exponent 12 in the original estimate to $6 + \epsilon$, where ϵ is any positive real number.

It is important to note that in our discussion of primality tests, we have only addressed *deterministic* algorithms, that is, algorithms that decide with certainty whether an integer is prime. In Chapter 6, we will introduce the notion of probabilistic primality tests, that is, tests that tell us that there is a high probability, but not a certainty, that an integer is prime.

3.1 Exercises

1. Determine which of the following integers are primes.

   a) 101 c) 107 e) 113
   b) 103 d) 111 f) 121

2. Determine which of the following integers are primes.

   a) 201 c) 207 e) 213
   b) 203 d) 211 f) 221

3. Use the sieve of Eratosthenes to find all primes less than 150.

4. Use the sieve of Eratosthenes to find all primes less than 200.

5. Find all primes that are the difference of the fourth powers of two integers.

6. Show that no integer of the form $n^3 + 1$ is a prime, other than $2 = 1^3 + 1$.

7. Show that if a and n are positive integers with $n > 1$ and $a^n - 1$ is prime, then $a = 2$ and n is prime. (*Hint:* Use the identity $a^{kl} - 1 = (a^k - 1)(a^{k(l-1)} + a^{k(l-2)} + \cdots + a^k + 1)$.)

8. (This exercise constructs another proof of the infinitude of primes.) Show that the integer $Q_n = n! + 1$, where n is a positive integer, has a prime divisor greater than n. Conclude that there are infinitely many primes.

9. Can you show that there are infinitely many primes by looking at the integers $S_n = n! - 1$, where n is a positive integer?

10. Using Euclid's proof that there are infinitely many primes, show that the nth prime p_n does not exceed $2^{2^{n-1}}$ whenever n is a positive integer. Conclude that when n is a positive integer, there are at least $n + 1$ primes less than 2^{2^n}.

11. Let $Q_n = p_1 p_2 \cdots p_n + 1$, where $p_1, p_2, \ldots, p_n$ are the n smallest primes. Determine the smallest prime factor of Q_n for $n = 1, 2, 3, 4, 5$, and 6. Do you think that Q_n is prime infinitely often? (*Note:* This is an unresolved question.)

12. Show that if p_k is the kth prime, where k is a positive integer, then $p_n \leq p_1 p_2 \cdots p_{n-1} + 1$ for all integers n with $n \geq 3$.

13. Show that if the smallest prime factor p of the positive integer n exceeds $\sqrt[3]{n}$, then n/p must be prime or 1.

14. Show that if p is a prime in the arithmetic progression $3n + 1, n = 1, 2, 3, \ldots$, then it is also in the arithmetic progression $6n + 1, n = 1, 2, 3, \ldots$.

15. Find the smallest prime in the arithmetic progression $an + b$, where

a) $a = 3, b = 1$. b) $a = 5, b = 4$. c) $a = 11, b = 16$.

16. Find the smallest prime in the arithmetic progression $an + b$, where

a) $a = 5, b = 1$. b) $a = 7, b = 2$. c) $a = 23, b = 13$.

17. Use the second principle of mathematical induction to prove that every integer greater than 1 is either prime or the product of two or more primes.

* **18.** Use the principle of inclusion–exclusion (Exercise 16 of Appendix B) to show that

$$\pi(n) = (\pi(\sqrt{n}) - 1) + n - \left(\left[\frac{n}{p_1}\right] + \left[\frac{n}{p_2}\right] + \cdots + \left[\frac{n}{p_r}\right]\right)$$
$$+ \left(\left[\frac{n}{p_1p_2}\right] + \left[\frac{n}{p_1p_3}\right] + \cdots + \left[\frac{n}{p_{r-1}p_r}\right]\right)$$
$$- \left(\left[\frac{n}{p_1p_2p_3}\right] + \left[\frac{n}{p_1p_2p_4}\right] + \cdots + \left[\frac{n}{p_{r-2}p_{r-1}p_r}\right]\right) + \cdots,$$

where $p_1, p_2, \ldots, p_r$ are the primes less than or equal to $\sqrt{n}$ (with $r = \pi(\sqrt{n})$). (*Hint:* Let property P_i be the property that an integer is divisible by p_i.)

19. Use Exercise 18 to find $\pi(250)$.

20. Show that $x^2 - x + 41$ is prime for all integers x with $0 \leq x \leq 40$. Show, however, that it is composite for $x = 41$.

21. Show that $2n^2 + 11$ is prime for all integers n with $0 \leq n \leq 10$, but is composite for $n = 11$.

22. Show that $2n^2 + 29$ is prime for all integers n with $0 \leq n \leq 28$, but is composite for $n = 29$.

* **23.** Show that if $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, where the coefficients are integers, then there is an integer y such that $f(y)$ is composite. (*Hint:* Assume that $f(x) = p$ is prime, and show that p divides $f(x + kp)$ for all integers k. Conclude that there is an integer y such that $f(y)$ is composite from the fact that a polynomial of degree $n, n > 1$, takes on each value at most n times.)

The *lucky numbers* are generated by the following sieving process: Start with the positive integers. Begin the process by crossing out every second integer in the list, starting your count with the integer 1. Other than 1, the smallest integer not crossed out is 3, so we continue by crossing out every third integer left, starting the count with the integer 1. The next integer left is 7, so we cross out every seventh integer left. Continue this process, where at each stage we cross out every kth integer left, where k is the smallest integer not crossed out, other than 1, not yet used in the sieving process. The integers that remain are the lucky numbers.

24. Find all lucky numbers less than 100.

25. Show that there are infinitely many lucky numbers.