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.

to date is that there are infinitely many integers n for which $n^2 + 1$ is either a prime or the product of two primes. This was shown by Henryk Iwaniec in 1973. Conjectures such as the $n^2 + 1$ conjecture may be easy to state, but are sometimes extremely difficult to resolve (see [Ri96] for more information).

3.2 Exercises

1. Find the smallest five consecutive composite integers.
2. Find one million consecutive composite integers.
3. Show that there are no "prime triplets," that is, primes p, $p + 2$, and $p + 4$, other than 3, 5 , and 7.
4. Find the smallest four sets of prime triplets of the form p, $p + 2$, $p + 6$.
5. Find the smallest four sets of prime triplets of the form p, $p + 4$, $p + 6$.
6. Find the smallest prime between n and $2n$ when n is

   a) 3. c) 19.
   b) 5. d) 31.

7. Find the smallest prime between n and $2n$ when n is

   a) 4. c) 23.
   b) 6. d) 47.

An unsettled conjecture asserts that for every positive integer n there is a prime between n^2 and $(n + 1)^2$.

8. Find the smallest prime between n^2 and $(n + 1)^2$ for all positive integers n with $n \leq 10$.
9. Find the smallest prime between n^2 and $(n + 1)^2$ for all positive integers n with $11 \leq n \leq 20$.
10. Verify Goldbach's conjecture for each of the following values of n.

    a) 50 c) 102 e) 200
    b) 98 d) 144 f) 222

CHRISTIAN GOLDBACH (1690–1764) was born in Königsberg, Prussia (the city noted in mathematical circles for its famous bridge problem). He became professor of mathematics at the Imperial Academy of St. Petersburg in 1725. In 1728, Goldbach went to Moscow to tutor Tsarevich Peter II. In 1742, he entered the Russian Ministry of Foreign Affairs as a staff member. Goldbach is most noted for his correspondence with eminent mathematicians, in particular Leonhard Euler and Daniel Bernoulli. Besides his well-known conjectures that every even positive integer greater than 2 is the sum of two primes and that every odd positive integer greater than 5 is the sum of three primes, Goldbach made several notable contributions to analysis.

6. Let a be a positive integer. What is the greatest common divisor of a and $a + 2$?

7. Show that if a and b are integers, not both 0, and c is a nonzero integer, then $(ca, cb) = |c|(a, b)$.

8. Show that if a and b are integers with $(a, b) = 1$, then $(a + b, a - b) = 1$ or 2.

9. What is $(a^2 + b^2, a + b)$, where a and b are relatively prime integers that are not both 0?

10. Show that if a and b are both even integers that are not both 0, then $(a, b) = 2(a/2, b/2)$.

11. Show that if a is an even integer and b is an odd integer, then $(a, b) = (a/2, b)$.

12. Show that if a, b, and c are integers such that $(a, b) = 1$ and $c \mid (a + b)$, then $(c, a) = (c, b) = 1$.

13. Show that if a, b, and c are mutually relatively prime nonzero integers, then $(a, bc) = (a, b)(a, c)$.

14. a) Show that if a, b, and c are integers with $(a, b) = (a, c) = 1$, then $(a, bc) = 1$.
    b) Use mathematical induction to show that if $a_1, a_2, \ldots, a_n$ are integers, and b is another integer such that $(a_1, b) = (a_2, b) = \cdots = (a_n, b) = 1$, then $(a_1 a_2 \cdots a_n, b) = 1$.

15. Find a set of three integers that are mutually relatively prime, but any two of which are not relatively prime. Do not use examples from the text.

16. Find four integers that are mutually relatively prime such that any three of these integers are not mutually relatively prime.

17. Find the greatest common divisor of each of the following sets of integers.

    a) 8, 10, 12
    b) 5, 25, 75
    c) 99, 9999, 0
    d) 6, 15, 21
    e) -7, 28, -35
    f) 0, 0, 1001

18. Find three mutually relatively prime integers from among the integers 66, 105, 42, 70, and 165.

19. Show that if $a_1, a_2, \ldots, a_n$ are integers that are not all 0 and c is a positive integer, then $(ca_1, ca_2, \ldots, ca_n) = c(a_1, a_2 \ldots, a_n)$.

20. Show that the greatest common divisor of the integers $a_1, a_2, \ldots, a_n$, not all 0, is the least positive integer that is a linear combination of $a_1, a_2, \ldots, a_n$.

21. Show that if k is an integer, then the integers $6k - 1$, $6k + 1$, $6k + 2$, $6k + 3$, and $6k + 5$ are pairwise relatively prime.

22. Show that if k is a positive integer, then $3k + 2$ and $5k + 3$ are relatively prime.

23. Show that $8a + 3$ and $5a + 2$ are relatively prime for all integers a.

24. Show that if a and b are relatively prime integers, then $(a + 2b, 2a + b) = 1$ or 3.

25. Show that every positive integer greater than 6 is the sum of two relatively prime integers greater than 1.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	−1
3	36	18	2	0	−3	4
4					4	−5

The values of s_j and t_j, $j = 0, 1, 2, 3, 4$, are computed as follows:

$$s_0 = 1, \qquad t_0 = 0,$$
$$s_1 = 0, \qquad t_1 = 1,$$
$$s_2 = s_0 - s_1q_1 = 1 - 0 \cdot 1 = 1, \qquad t_2 = t_0 - t_1q_1 = 0 - 1 \cdot 1 = -1,$$
$$s_3 = s_1 - s_2q_2 = 0 - 1 \cdot 3 = -3, \qquad t_3 = t_1 - t_2q_2 = 1 - (-1)3 = 4,$$
$$s_4 = s_2 - s_3q_3 = 1 - (-3) \cdot 1 = 4, \qquad t_4 = t_2 - t_3q_3 = -1 - 4 \cdot 1 = -5.$$

Because $r_4 = 18 = (252, 198)$ and $r_4 = s_4a + t_4b$, we have

$$18 = (252, 198) = 4 \cdot 252 - 5 \cdot 198.$$ ◀

Note that the greatest common divisor of two integers may be expressed as a linear combination of these integers in an infinite number of ways. To see this, let $d = (a, b)$ and let $d = sa + tb$ be one way to write d as a linear combination of a and b, guaranteed to exist by the previous discussion. Then for all integers k,

$$d = (s + k(b/d))a + (t - k(a/d))b.$$

Example 3.15. With $a = 252$ and $b = 198$, we have $18 = (252, 198) = (4 + 11k)252 + (-5 - 14k)198$ for any integer k. ◀

3.4 Exercises

1. Use the Euclidean algorithm to find each of the following greatest common divisors.

   a) (45, 75) c) (666, 1414)
   b) (102, 222) d) (20785, 44350)

2. Use the Euclidean algorithm to find each of the following greatest common divisors.

   a) (51, 87) c) (981, 1234)
   b) (105, 300) d) (34709, 100313)

3. For each pair of integers in Exercise 1, express the greatest common divisor of the integers as a linear combination of these integers.

4. For each pair of integers in Exercise 2, express the greatest common divisor of the integers as a linear combination of these integers.

5. Find the greatest common divisor of each of the following sets of integers.

   a) 6, 10, 15 b) 70, 98, 105 c) 280, 330, 405, 490

14. Use the least-remainder algorithm to find (384, 226).

15. Show that the least-remainder algorithm always produces the greatest common divisor of two integers.

** **16.** Show that the least-remainder algorithm is always at least as fast as the Euclidean algorithm. (*Hint:* First show that if a and b are positive integers with $2b < a$, then the least-remainder algorithm can find (a, b) with no more steps than it uses to find $(a, a - b)$.)

* **17.** Find a sequence of integers $v_0, v_1, v_2, \ldots$, such that the least-remainder algorithm takes exactly n divisions to find (v_{n+1}, v_{n+2}).

* **18.** Show that the number of divisions needed to find the greatest common divisor of two positive integers using the least-remainder algorithm is less than 8/3 times the number of digits in the smaller of the two numbers, plus 4/3.

* **19.** Let m and n be positive integers and let a be an integer greater than 1. Show that $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

* **20.** Show that if m and n are positive integers, then $(f_m, f_n) = f_{(m,n)}$.

The next two exercises deal with the *game of Euclid*. Two players begin with a pair of positive integers and take turns making moves of the following type. A player can move from the pair of positive integers $\{x, y\}$ with $x \geq y$, to any of the pairs $\{x - ty, y\}$, where t is a positive integer and $x - ty \geq 0$. A *winning move* consists of moving to a pair with one element equal to 0.

21. Show that every sequence of moves starting with the pair $\{a, b\}$ must eventually end with the pair $\{0, (a, b)\}$.

* **22.** Show that in a game beginning with the pair $\{a, b\}$, the first player may play a winning strategy if $a = b$ or if $a > b(1 + \sqrt{5})/2$; otherwise, the second player may play a winning strategy. (*Hint:* First show that if $y < x \leq y(1 + \sqrt{5})/2$, then there is a unique move from $\{x, y\}$ that goes to a pair $\{z, y\}$ with $y > z(1 + \sqrt{5})/2$.)

* **23.** Show that the number of bit operations needed to use the Euclidean algorithm to find the greatest common divisor of two positive integers a and b with $a > b$ is $O((\log_2 a)^2)$. (*Hint:* First show that the complexity of division of the positive integer q by the positive integer d is $O(\log d \log q)$.)

* **24.** Let a and b be positive integers and let r_j and q_j, $j = 1, 2, \ldots, n$ be the remainders and quotients of the steps of the Euclidean algorithm as defined in this section.

a) Find the value of $\sum_{j=1}^{n} r_j q_j$.

b) Find the value of $\sum_{j=1}^{n} r_j^2 q_j$.

25. Suppose that a and b are positive integers with $a \geq b$. Let q_i and r_i be the quotients and remainders in the steps of the Euclidean algorithm for $i = 1, 2, \ldots, n$, where r_n is the last nonzero remainder. Let $Q_i = \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}$ and $Q = \prod_{i=0}^{n} Q_i$. Show that $\begin{pmatrix} a \\ b \end{pmatrix} = Q \begin{pmatrix} r_n \\ 0 \end{pmatrix}$.