Example 6.6. To find $2^{9!} \pmod{5,157,437}$, we perform the following sequence of computations:

$$r_2 \equiv r_1^2 = 2^2 \equiv 4 \pmod{5,157,437}$$
$$r_3 \equiv r_2^3 = 4^3 \equiv 64 \pmod{5,157,437}$$
$$r_4 \equiv r_3^4 = 64^4 \equiv 1,304,905 \pmod{5,157,437}$$
$$r_5 \equiv r_4^5 = 1,304,905^5 \equiv 404,913 \pmod{5,157,437}$$
$$r_6 \equiv r_5^6 = 404,913^6 \equiv 2,157,880 \pmod{5,157,437}$$
$$r_7 \equiv r_6^7 = 2,157,880^7 \equiv 4,879,227 \pmod{5,157,437}$$
$$r_8 \equiv r_7^8 = 4,879,227^8 \equiv 4,379,778 \pmod{5,157,437}$$
$$r_9 \equiv r_8^9 = 4,379,778^9 \equiv 4,381,440 \pmod{5,157,437}.$$

It follows that $2^{9!} \equiv 4,381,440 \pmod{5,157,437}$. ◀

The following example illustrates the use of the Pollard $p-1$ method to find a factor of the integer 5,157,437.

Example 6.7. To factor 5,157,437 using the Pollard $p-1$ method, we successively find r_k, the least positive residue of $2^{k!}$ modulo 5,157,437, for $k = 1, 2, 3, \ldots$, as was done in Example 6.6. We compute $(r_k - 1, 5,157,437)$ at each step. To find a factor of 5,157,437 requires nine steps, because $(r_k - 1, 5,157,437) = 1$ for $k = 1, 2, 3, 4, 5, 6, 7, 8$ (as the reader can verify), but $(r_9 - 1, 5,157,437) = (4,381,439, 5,157,437) = 2269$. It follows that 2269 is a divisor of 5,157,437. ◀

The Pollard $p-1$ method does not always work. However, because nothing in the method depends on the choice of 2 as the base, we can extend the method and find a factor for more integers by using integers other than 2 as the base. In practice, the Pollard $p-1$ method is used after trial divisions by small primes, but before the heavy artillery of such methods as the quadratic sieve and the elliptic curve method.

6.1 Exercises

1. Show that $10! + 1$ is divisible by 11, by grouping together pairs of inverses modulo 11 that occur in 10!.
2. Show that $12! + 1$ is divisible by 13, by grouping together pairs of inverses modulo 13 that occur in 12!.
3. What is the remainder when 16! is divided by 19?
4. What is the remainder when 5!25! is divided by 31?
5. Using Wilson's theorem, find the least positive residue of $8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13$ modulo 7.
6. What is the remainder when $7 \cdot 8 \cdot 9 \cdot 15 \cdot 16 \cdot 17 \cdot 23 \cdot 24 \cdot 25 \cdot 43$ is divided by 11?

7. What is the remainder when 18! is divided by 437?
8. What is the remainder when 40! is divided by 1763?
9. What is the remainder when 5^{100} is divided by 7?
10. What is the remainder when 6^{2000} is divided by 11?
11. Using Fermat's little theorem, find the least positive residue of $3^{999,999,999}$ modulo 7.
12. Using Fermat's little theorem, find the least positive residue of $2^{1000000}$ modulo 17.
13. Show that $3^{10} \equiv 1 \pmod{11^2}$.
14. Using Fermat's little theorem, find the last digit of the base 7 expansion of 3^{100}.
15. Using Fermat's little theorem, find the solutions of the following linear congruences.
    a) $7x \equiv 12 \pmod{17}$ b) $4x \equiv 11 \pmod{19}$
16. Show that if n is a composite integer with $n \neq 4$, then $(n-1)! \equiv 0 \pmod{n}$.
17. Show that if p is an odd prime, then $2(p-3)! \equiv -1 \pmod{p}$.
18. Show that if n is odd and $3 \nmid n$, then $n^2 \equiv 1 \pmod{24}$.
19. Show that $a^{12} - 1$ is divisible by 35 whenever $(a, 35) = 1$.
20. Show that $a^6 - 1$ is divisible by 168 whenever $(a, 42) = 1$.
21. Show that $42 \mid (n^7 - n)$ for all positive integers n.
22. Show that $30 \mid (n^9 - n)$ for all positive integers n.
23. Show that $1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{(p-1)} \equiv -1 \pmod{p}$ whenever p is prime. (It has been conjectured that the converse of this is also true.)
24. Show that $1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 0 \pmod{p}$ when p is an odd prime.
25. Show that if p is prime and a and b are integers not divisible by p, with $a^p \equiv b^p \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$.
26. Use the Pollard $p-1$ method to find a divisor of 689.
27. Use the Pollard $p-1$ method to find a divisor of 7,331,117. (For this exercise, you will need to use either a calculator or computational software.)
28. Show that if p and q are distinct primes, then $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.
29. Show that if p is prime and a is an integer, then $p \mid (a^p + (p-1)!\,a)$.
30. Show that if p is an odd prime, then $1^2 3^2 \cdots (p-4)^2 (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$.
31. Show that if p is prime and $p \equiv 3 \pmod{4}$, then $((p-1)/2)! \equiv \pm 1 \pmod{p}$.
32. a) Let p be prime, and suppose that r is a positive integer less than p such that $(-1)^r r! \equiv -1 \pmod{p}$. Show that $(p-r+1)! \equiv -1 \pmod{p}$.
    b) Using part (a), show that $61! \equiv 63! \equiv -1 \pmod{71}$.
33. Using Wilson's theorem, show that if p is a prime and $p \equiv 1 \pmod{4}$, then the congruence $x^2 \equiv -1 \pmod{p}$ has two incongruent solutions given by $x \equiv \pm((p-1)/2)! \pmod{p}$.

34. Show that if p is a prime and $0 < k < p$, then $(p-k)!(k-1)! \equiv (-1)^k \pmod{p}$.

35. Show that if n is an integer, then

$$\pi(n) = \sum_{j=2}^{n} \left[\frac{(j-1)!+1}{j} - \left[\frac{(j-1)!}{j} \right] \right].$$

* **36.** For which positive integers n is $n^4 + 4^n$ prime?

37. Show that the pair of positive integers n and $n+2$ are twin primes if and only if $4((n-1)!+1)+n \equiv 0 \pmod{n(n+2)}$, where $n \neq 1$.

38. Show that if the positive integers n and $n+k$, where $n > k$ and k is an even positive integer, are both prime, then $(k!)^2((n-1)!+1)+n(k!-1)(k-1)! \equiv 0 \pmod{n(n+k)}$.

39. Show that if p is prime, then $\binom{2p}{p} \equiv 2 \pmod{p}$.

40. Exercise 74 of Section 3.5 shows that if p is prime and k is a positive integer less than p, then the binomial coefficient $\binom{p}{k}$ is divisible by p. Use this fact and the binomial theorem to show that if a and b are integers, then $(a+b)^p \equiv a^p + b^p \pmod{p}$.

41. Prove Fermat's little theorem by mathematical induction. (*Hint:* In the induction step, use Exercise 40 to obtain a congruence for $(a+1)^p$.)

* **42.** Using Exercise 30 of Section 4.3, prove *Gauss's generalization of Wilson's theorem*, namely that the product of all the positive integers less than m that are relatively prime to m is congruent to 1 (mod m), unless $m = 4$, p^t, or $2p^t$, where p is an odd prime and t is a positive integer, in which case it is congruent to -1 (mod m).

43. A deck of cards is shuffled by cutting the deck into two piles of 26 cards. Then, the new deck is formed by alternating cards from the two piles, starting with the bottom pile.

a) Show that if a card begins in the cth position in the deck, it will be in the bth position in the new deck, where $b \equiv 2c \pmod{53}$ and $1 \leq b \leq 52$.

b) Determine the number of shuffles of the type described above that are needed to return the deck of cards to its original order.

44. Let p be prime and let a be a positive integer not divisible by p. We define the *Fermat quotient* $q_p(a)$ by $q_p(a) = (a^{p-1} - 1)/p$. Show that if a and b are positive integers not divisible by the prime p, then $q_p(ab) \equiv q_p(a) + q_p(b) \pmod{p}$.

45. Let p be prime and let $a_1, a_2, \ldots, a_p$ and $b_1, b_2, \ldots, b_p$ be complete systems of residues modulo p. Show that $a_1b_1, a_2b_2, \ldots, a_pb_p$ is not a complete system of residues modulo p.

* **46.** Show that if n is a positive integer with $n \geq 2$, then n does not divide $2^n - 1$.

* **47.** Let p be an odd prime. Show that $(p-1)!^{p^{n-1}} \equiv -1 \pmod{p^n}$.

48. Show that if p is a prime with $p > 5$, then $(p-1)!+1$ has at least two different prime divisors.

49. Show that if a and n are relatively prime integers with $n > 1$, then n is prime if and only if $(x-a)^n$ and $x^n - a$ are congruent modulo n as polynomials. (Recall from the preamble to Exercise 40 in Section 4.1 that two polynomials are congruent modulo n as

Example 6.20. We know that $2^{\phi(9)-1} = 2^{6-1} = 2^5 = 32 \equiv 5 \pmod 9$ is an inverse of 2 modulo 9. ◀

We can solve linear congruences using this observation. To solve $ax \equiv b \pmod m$, where $(a, m) = 1$, we multiply both sides of this congruence by $a^{\phi(m)-1}$ to obtain

$$a^{\phi(m)-1}ax \equiv a^{\phi(m)-1}b \pmod m.$$

Therefore, the solutions are those integers x such that $x \equiv a^{\phi(m)-1}b \pmod m$.

Example 6.21. The solutions of $3x \equiv 7 \pmod{10}$ are given by $x \equiv 3^{\phi(10)-1} \cdot 7 \equiv 3^3 \cdot 7 \equiv 9 \pmod{10}$, because $\phi(10) = 4$. ◀

6.3 Exercises

1. Find a reduced residue system modulo each of the following integers.

   a) 6 b) 9 c) 10 d) 14 e) 16 f) 17

2. Find a reduced residue system modulo 2^m, where m is a positive integer.

3. Show that if $c_1, c_2, \ldots, c_{\phi(m)}$ is a reduced residue system modulo m, where m is a positive integer with $m \neq 2$, then $c_1 + c_2 + \cdots + c_{\phi(m)} \equiv 0 \pmod m$.

4. Show that if a and m are positive integers with $(a, m) = (a - 1, m) = 1$, then $1 + a + a^2 + \ldots + a^{\phi(m)-1} \equiv 0 \pmod m$.

5. Find the last digit of the decimal expansion of 3^{1000}.

6. Find the last digit of the decimal expansion of $7^{999,999}$.

7. Use Euler's theorem to find the least positive residue of $3^{100,000}$ modulo 35.

8. Show that if a is an integer such that a is not divisible by 3 or such that a is divisible by 9, then $a^7 \equiv a \pmod{63}$.

9. Show that if a is an integer relatively prime to 32,760, then $a^{12} \equiv 1 \pmod{32{,}760}$.

10. Show that $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$, if a and b are relatively prime positive integers.

11. Solve each of the following linear congruences using Euler's theorem.

    a) $5x \equiv 3 \pmod{14}$ b) $4x \equiv 7 \pmod{15}$ c) $3x \equiv 5 \pmod{16}$

12. Show that the solutions to the simultaneous system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r}, \end{aligned}$$

    where the m_j are pairwise relatively prime, are given by

$$x \equiv a_1 M_1^{\phi(m_1)} + a_2 M_2^{\phi(m_2)} + \cdots + a_r M_r^{\phi(m_r)} \pmod M,$$

    where $M = m_1 m_2 \cdots m_r$ and $M_j = M/m_j$ for $j = 1, 2, \ldots, r$.

13. Use Exercise 12 to solve each of the systems of congruences in Exercise 4 of Section 4.3.

14. Use Exercise 12 to solve the system of congruences in Exercise 5 of Section 4.3.

15. Use Euler's theorem to find the last digit in the decimal expansion of 7^{1000}.

16. Use Euler's theorem to find the last digit in the hexadecimal expansion of $5^{1,000,000}$.

17. Find $\phi(n)$ for the integers n with $13 \leq n \leq 20$.

18. Show that every positive integer relatively prime to 10 divides infinitely many repunits (see the preamble to Exercise 11 of Section 5.1). (*Hint:* Note that the n-digit repunit $111\ldots11 = (10^n - 1)/9$.)

19. Show that every positive integer relatively prime to b divides infinitely many base b repunits (see the preamble to Exercise 15 of Section 5.1).

* 20. Show that if m is a positive integer, $m > 1$, then $a^m \equiv a^{m-\phi(m)} \pmod{m}$ for all positive integers a.

6.3 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica*, or programs you have written, carry out the following computations and explorations.

1. Find $\phi(n)$ for all integers n less than 1000. What conjectures can you make about the values of $\phi(n)$?

2. Let $\Phi(n) = \sum_{i=1}^{n} \phi(n)$. Investigate the value of $\Phi(n)/n^2$ for increasingly large values of n, such as $n = 100$, $n = 1000$, and $n = 10{,}000$. Can you make a conjecture about the limit of this ratio as n grows large without bound?

Programming Projects

Write programs using Maple, *Mathematica*, or a language of your choice to do the following.

1. Construct a reduced residue system modulo n for a given positive integer n.

2. Solve linear congruences using Euler's theorem.

3. Find the solutions of a simultaneous system of linear congruences using Euler's theorem and the Chinese remainder theorem (see Exercise 12).

the equation $\phi(n) = 8$ implies that no prime exceeding 9 divides n (otherwise $\phi(n) > p_j - 1 > 8$). Furthermore, 7 cannot divide n because if it did, $7 - 1 = 6$ would be a factor of $\phi(n)$. It follows that $n = 2^a 3^b 5^c$, where a, b, and c are nonnegative integers. We can also conclude that $b = 0$ or $b = 1$ and that $c = 0$ or $c = 1$; otherwise, 3 or 5 would divide $\phi(n) = 8$.

To find all solutions we need only consider four cases. When $b = c = 0$, we have $n = 2^a$, where $a \geq 1$. This implies that $\phi(n) = 2^{a-1}$, which means that $a = 4$ and $n = 16$. When $b = 0$ and $c = 1$, we have $n = 2^a \cdot 5$, where $a \geq 1$. This implies that $\phi(n) = 2^{a-1} \cdot 4$, so $a = 2$ and $n = 20$. When $b = 1$ and $c = 0$, we have $n = 2^a \cdot 3$, where $a \geq 1$. This implies that $\phi(n) = 2^{a-1} \cdot 2 = 2^a$, so $a = 3$ and $n = 24$. Finally, when $b = 1$ and $c = 1$, we have $n = 2^a \cdot 3 \cdot 5$. We need to consider the case where $a = 0$, as well as the case where $a \geq 1$. When $a = 0$, we have $n = 15$, which is a solution because $\phi(15) = 8$. When $a \geq 1$, we have $\phi(n) = 2^{a-1} \cdot 2 \cdot 4 = 2^{a+2}$. This means that $a = 1$ and $n = 30$. Putting everything together, we see that all the solutions to $\phi(n) = 8$ are $n = 15, 16, 20, 24$ and 30. ◀

7.1 Exercises

1. Determine whether each of the following arithmetic functions is completely multiplicative. Prove your answers.

   a) $f(n) = 0$ d) $f(n) = \log n$ g) $f(n) = n + 1$
   b) $f(n) = 2$ e) $f(n) = n^2$ h) $f(n) = n^n$
   c) $f(n) = n/2$ f) $f(n) = n!$ i) $f(n) = \sqrt{n}$

2. Find the value of the Euler phi-function at each of the following integers.

   a) 100 d) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$
   b) 256 e) 10!
   c) 1001 f) 20!

3. Show that $\phi(5186) = \phi(5187) = \phi(5188)$.

4. Find all positive integers n such that $\phi(n)$ has each of the following values. Be sure to prove that you have found all solutions.

   a) 1 b) 2 c) 3 d) 4

5. Find all positive integers n such that $\phi(n) = 6$. Be sure to prove that you have found all solutions.

6. Find all positive integers n such that $\phi(n) = 12$. Be sure to prove that you have found all solutions.

7. Find all positive integers n such that $\phi(n) = 24$. Be sure to prove that you have found all solutions.

8. Show that there is no positive integer n such that $\phi(n) = 14$.

9. Can you find a rule involving the Euler phi-function for producing the terms of the sequence $1, 2, 2, 4, 4, 4, 6, 8, 6, \ldots$?

10. Can you find a rule involving the Euler phi-function for producing the terms of the sequence $2, 3, 0, 4, 0, 4, 0, 5, 0, \ldots$?

11. For which positive integers n does $\phi(3n) = 3\phi(n)$?

12. For which positive integers n is $\phi(n)$ divisible by 4?

13. For which positive integers n is $\phi(n)$ equal to $n/2$?

14. For which positive integers n does $\phi(n) \mid n$?

15. Show that if n is a positive integer, then

$$\phi(2n) = \begin{cases} \phi(n) & \text{if } n \text{ is odd;} \\ 2\phi(n) & \text{if } n \text{ is even.} \end{cases}$$

16. Show that if n is a positive integer having k distinct odd prime divisors, then $\phi(n)$ is divisible by 2^k.

17. For which positive integers n is $\phi(n)$ a power of 2?

18. Show that if n is an odd integer, then $\phi(4n) = 2\phi(n)$.

19. Show that if $n = 2\phi(n)$, where n is a positive integer, then $n = 2^j$ for some positive integer j.

20. Let p be prime. Show that $p \nmid n$, where n is a positive integer, if and only if $\phi(np) = (p-1)\phi(n)$.

21. Show that if m and n are positive integers and $(m, n) = p$, where p is prime, then $\phi(mn) = p\phi(m)\phi(n)/(p-1)$.

22. Show that if m and k are positive integers, then $\phi(m^k) = m^{k-1}\phi(m)$.

23. Show that if a and b are positive integers, then

$$\phi(ab) = (a, b)\phi(a)\phi(b)/\phi((a, b)).$$

Conclude that $\phi(ab) > \phi(a)\phi(b)$ when $(a, b) > 1$.

24. Find the least positive integer n such that the following hold.

a) $\phi(n) \geq 100$ c) $\phi(n) \geq 10{,}000$
b) $\phi(n) \geq 1000$ d) $\phi(n) \geq 100{,}000$

25. Use the Euler phi-function to show that there are infinitely many primes. (*Hint:* Assume there are only a finite number of primes $p_1, \ldots, p_k$. Consider the value of the Euler phi-function at the product of these primes.)

26. Show that if the equation $\phi(n) = k$, where k is a positive integer, has exactly one solution n, then $36 \mid n$.

27. Show that the equation $\phi(n) = k$, where k is a positive integer, has finitely many solutions in integers n whenever k is a positive integer.

28. Show that if p is prime, $2^a p + 1$ is composite for $a = 1, 2, \ldots, r$ and p is not a Fermat prime, where r is a positive integer, then $\phi(n) = 2^r p$ has no solution.

* 29. Show that there are infinitely many positive integers k such that the equation $\phi(n) = k$ has exactly two solutions, where n is a positive integer. (*Hint:* Take $k = 2 \cdot 3^{6j+1}$, where $j = 1, 2, \ldots$.)

30. Show that if n is a positive integer with $n \neq 2$ and $n \neq 6$, then $\phi(n) \geq \sqrt{n}$.

*** 31.** Show that if n is a composite positive integer and $\phi(n) \mid n - 1$, then n is square-free and is the product of at least three distinct primes.

32. Show that if m and n are positive integers with $m \mid n$, then $\phi(m) \mid \phi(n)$.

*** 33.** Prove Theorem 7.5, using the principle of inclusion-exclusion (see Exercise 16 of Appendix B).

34. Show that a positive integer n is composite if and only if $\phi(n) \leq n - \sqrt{n}$.

35. Let n be a positive integer. Define the sequence of positive integers $n_1, n_2, n_3, \ldots$ recursively by $n_1 = \phi(n)$ and $n_{k+1} = \phi(n_k)$ for $k = 1, 2, 3, \ldots$. Show that there is a positive integer r such that $n_r = 1$.

A multiplicative function is called *strongly multiplicative* if and only if $f(p^k) = f(p)$ for every prime p and every positive integer k.

36. Show that $f(n) = \phi(n)/n$ is a strongly multiplicative function.

Two arithmetic functions f and g may be multiplied using the *Dirichlet product*, which is defined by

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d).$$

37. Show that $f * g = g * f$.

38. Show that $(f * g) * h = f * (g * h)$.

We define the *ι function* by

$$\iota(n) = \begin{cases} 1 & \text{if } n = 1; \\ 0 & \text{if } n > 1. \end{cases}$$

39. a) Show that ι is a multiplicative function.

b) Show that $\iota * f = f * \iota = f$ for all arithmetic functions f.

40. The arithmetic function g is said to be the *inverse* of the arithmetic function f if $f * g = g * f = \iota$. Show that the arithmetic function f has an *inverse* if and only if $f(1) \neq 0$. Show that if f has an inverse it is unique. (*Hint:* When $f(1) \neq 0$, find the inverse f^{-1} of f by calculating $f^{-1}(n)$ recursively, using the fact that $\iota(n) = \sum_{d|n} f(d)f^{-1}(n/d)$.)

41. Show that if f and g are multiplicative functions, then the Dirichlet product $f * g$ is also multiplicative.

42. Show that if f and g are arithmetic functions, $F = f * g$, and h is the Dirichlet inverse of g, then $f = F * h$.

We define *Liouville's function* $\lambda(n)$, named after French mathematician *Joseph Liouville*, by $\lambda(1) = 1$, and for $n > 1$, $\lambda(n) = (-1)^{a_1+a_2+\cdots+a_m}$, where the prime-power factorization of n is $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$.

43. Find $\lambda(n)$ for each of the following values of n.

a) 12 c) 210 e) 1001 g) 20!
b) 20 d) 1000 f) 10!

44. Show that $\lambda(n)$ is completely multiplicative.

45. Show that if n is a positive integer, then $\sum_{d|n} \lambda(d)$ equals 0 if n is not a perfect square, and equals 1 if n is a perfect square.

46. Show that if f and g are multiplicative functions, then fg is also multiplicative, where $(fg)(n) = f(n)g(n)$ for every positive integer n.

47. Show that if f and g are completely multiplicative functions, then fg is also completely multiplicative.

48. Show that if f is completely multiplicative, then $f(n) = f(p_1)^{a_1} f(p_2)^{a_2} \cdots f(p_m)^{a_m}$, where the prime-power factorization of n is $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$.

A function f that satisfies the equation $f(mn) = f(m) + f(n)$ for all relatively prime positive integers m and n is called *additive*, and if the above equation holds for all positive integers m and n, f is called *completely additive*.

49. Show that the function $f(n) = \log n$ is completely additive.

The function $\omega(n)$ is the function that denotes the number of distinct prime factors of the positive integer n.

50. Find $\omega(n)$ for each of the following integers.

a) 1 b) 2 c) 20 d) 84 e) 128

JOSEPH LIOUVILLE (1809–1882), born in Saint-Omer, France, was the son of a captain in Napoleon's army. He studied mathematics at the Collège St. Louis in Paris, and in 1825 he enrolled in the École Polytechnique; after graduating, he entered the École des Ponts et Chaussées (School of Bridges and Roads). Health problems while working on engineering projects and his interest in theoretical topics convinced him to pursue an academic career. He left the École des Ponts et Chaussées in 1830, but during his time there he wrote papers on electrodynamics, the theory of heat, and partial differential equations.

Liouville's first academic appointment was as an assistant at the École Polytechnique in 1831. He had a teaching load of around 40 hours a week at several different institutions. Some of his less able students complained that he lectured at too high a level. In 1836, Liouville founded the *Journal de Mathématiques Pures et Appliquées*, which played an important role in French mathematics in the nineteenth century. In 1837, he was appointed to lecture at the Collège de France and the following year he was appointed Professor at the École Polytechnique. Besides his academic interests, Liouville was also involved in politics. He was elected to Constituting Assembly in 1848 as a moderate republican, but lost in the election of 1849, embittering him. Liouville was appointed to a chair at the Collège de France in 1851, and the chair of mechanics at the Faculté des Sciences in 1857. Around this time, his heavy teaching load began to take its toll. Liouville was a perfectionist and was unhappy when he could not devote sufficient time to his lectures.

Liouville's work covered many diverse areas of mathematics, including mathematical physics, astronomy, and many areas of pure mathematics. He was the first person to provide an explicit example of a transcendental number. He is also known today for what is now called Sturm-Liouville theory, used in the solution of integral equations, and he made important contributions to differential geometry. His total output exceeds 400 papers in the mathematical sciences, with nearly half of those in number theory alone.

inversion formula is that we can turn this statement around. That is, if the summatory function F of an arithmetic function f is multiplicative, then so is f.

Theorem 7.17. Let f be an arithmetic function with summatory $F = \sum_{d|n} f(d)$. Then, if F is multiplicative, f is also multiplicative.

Proof. Suppose that m and n are relatively prime positive integers. We want to show that $f(mn) = f(m)f(n)$. To show this, first note that by Lemma 3.7, if d is a divisor of mn, then $d = d_1d_2$ where $d_1 \mid m$, $d_2 \mid n$, and $(d_1, d_2) = 1$. Using the Möbius inversion formula and the fact that μ and F are multiplicative, we see that

$$\begin{aligned} f(mn) &= \sum_{d|mn} \mu(d) F\left(\frac{mn}{d}\right) \\ &= \sum_{d_1|m,\, d_2|n} \mu(d_1d_2) F\left(\frac{mn}{d_1d_2}\right) \\ &= \sum_{d_1|m,\, d_2|n} \mu(d_1)\mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right) \\ &= \sum_{d_1|m} \mu(d_1) F\left(\frac{m}{d_1}\right) \cdot \sum_{d_2|n} \mu(d_2) F\left(\frac{n}{d_2}\right) \\ &= f(m)f(n). \end{aligned}$$

■

7.4 Exercises

1. Find the following values of the Möbius function.

   a) $\mu(12)$ d) $\mu(50)$ g) $\mu(10!)$
   b) $\mu(15)$ e) $\mu(1001)$
   c) $\mu(30)$ f) $\mu(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13)$

2. Find the following values of the Möbius function.

   a) $\mu(33)$ d) $\mu(740)$ g) $\mu(10!/(5!)^2)$
   b) $\mu(105)$ e) $\mu(999)$
   c) $\mu(110)$ f) $\mu(3 \cdot 7 \cdot 13 \cdot 19 \cdot 23)$

3. Find the value of $\mu(n)$ for each integer n with $100 \le n \le 110$.
4. Find the value of $\mu(n)$ for each integer n with $1000 \le n \le 1010$.
5. Find all integers n, $1 \le n \le 100$ with $\mu(n) = 1$.
6. Find all composite integers n, $100 \le n \le 200$ with $\mu(n) = -1$.

The *Mertens function* $M(n)$ is defined by $M(n) = \sum_{i=1}^{n} \mu(i)$.

7. Find $M(n)$ for all positive integers not exceeding 10.
8. Find $M(n)$ for $n = 100$.

9. Show that $M(n)$ is the difference between the number of square-free positive integers not exceeding n with an even number of prime divisors and those with an odd number of prime divisors.

10. Show that if n is a positive integer, then $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$.

11. Prove or disprove that there are infinitely many positive integers n such that $\mu(n) + \mu(n+1) = 0$.

12. Prove or disprove that there are infinitely many positive integers n such that $\mu(n-1) + \mu(n) + \mu(n+1) = 0$.

13. For how many consecutive integers can the Möbius function $\mu(n)$ take a nonzero value?

14. For how many consecutive integers can the Möbius function $\mu(n)$ take the value 0?

15. Show that if n is a positive integer, then $\phi(n) = n \sum_{d|n} \mu(d)/d$. (*Hint:* Use the Möbius inversion formula.)

16. Use the Möbius inversion formula and the identity $n = \sum_{d|n} \phi(n/d)$, demonstrated in Section 7.1, to show the following.
    a) $\phi(p^t) = p^t - p^{t-1}$, whenever p is prime and t is a positive integer.
    b) $\phi(n)$ is multiplicative.

17. Suppose that f is a multiplicative function with $f(1) = 1$. Show that

$$\sum_{d|n} \mu(d) f(d) = (1 - f(p_1))(1 - f(p_2)) \cdots (1 - f(p_k)),$$

    where $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the prime-power factorization of n.

18. Use Exercise 17 to find a simple formula for $\sum_{d|n} d\mu(d)$ for all positive integers n.

19. Use Exercise 17 to find a simple formula for $\sum_{d|n} \mu(d)/d$ for all positive integers n.

20. Use Exercise 17 to find a simple formula for $\sum_{d|n} \mu(d)\tau(d)$ for all positive integers n.

21. Use Exercise 17 to find a simple formula for $\sum_{d|n} \mu(d)\sigma(d)$ for all positive integers n.

22. Let n be a positive integer. Show that

$$\prod_{d|n} \mu(d) = \begin{cases} -1 & \text{if } n \text{ is a prime;} \\ 0 & \text{if } n \text{ has a square factor;} \\ 1 & \text{if } n \text{ is square-free and composite.} \end{cases}$$

23. Show that

$$\sum_{d|n} \mu^2(d) = 2^{\omega(n)},$$

    where $\omega(n)$ denotes the number of distinct prime factors of n.

24. Use Exercise 23 and the Möbius inversion formula to show that

$$\mu^2(n) = \sum_{d|n} \mu(d) 2^{\omega(n/d)}.$$

25. Show that $\sum_{d|n} \mu(d)\lambda(d) = 2^{\omega(n)}$ for all positive integers n, where $\omega(n)$ is the number of distinct prime factors of n. (See the preamble to Exercise 43 in Section 7.1 for a definition of $\lambda(n)$.)

26. Show that $\sum_{d|n} \lambda(n/d)2^{\omega(d)} = 1$ for all positive integers n.

Exercises 27–29 provide a proof of the Möbius inversion formula and Theorem 7.17 using the concepts of the Dirichlet product and the Dirichlet inverse, defined in the exercise set of Section 7.1.

27. Show that the Möbius function $\mu(n)$ is the Dirichlet inverse of the function $\nu(n) = 1$.

28. Use Exercise 38 in Section 7.1 and Exercise 27 to prove the Möbius inversion formula.

29. Prove Theorem 7.17 by noting that if $F = f \star \nu$, where $\nu = 1$ for all positive integers n, then $f = F \star \mu$.

The *Mangoldt function* Λ is defined for all positive integers n by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, \text{ where } p \text{ is prime and } k \text{ is a positive integer;} \\ 0 & \text{otherwise.} \end{cases}$$

30. Show that $\sum_{d|n} \Lambda(d) = \log n$ whenever n is a positive integer.

31. Use the Möbius inversion formula and Exercise 30 to show that

$$\Lambda(n) = -\sum_{d|n} \mu(d) \log d.$$

7.4 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica*, or programs you have written, carry out the following computations and explorations.

1. Find $\mu(n)$ for each of the following values of n.

   a) 421,602,180,943 b) 186,728,732,190 c) 737,842,183,177

2. Find $M(n)$, the value of the Mertens function at n, for each of the following integers. (See the preamble to Exercise 7 for the definition of $M(n)$.)

   a) 1000 b) 10,000 c) 100,000

3. A famous conjecture made in 1897 by F. Mertens, and disproved in 1985 by A. Odlyzko and H. te Riele (in [Odte85]), was that $|M(n)| < \sqrt{n}$ for all positive integers n, where $M(n)$ is the Mertens function. Show that this conjecture, called Mertens' conjecture, is true for all integers n for as large a range as you can. Do not expect to find a counterexample, because the smallest n for which the conjecture is false is fantastically large. What is known is that there is a counterexample less than $3.21 \cdot 10^{64}$. Before the conjecture was shown to be false, it had been checked by computer for all integers n up to 10^{10}. This shows that even a tremendous amount of evidence can be misleading, because the smallest counterexample to a conjecture can nevertheless be titanically large.

2. Simplify each of the following expressions, expressing your answer in the form of a Gaussian integer $a + bi$.

a) $(-1+i)^3(1+i)^3$ b) $(3+2i)(3-i)^2$ c) $(2+i)^2(5-i)^3$

3. Determine whether the Gaussian integer α divides the Gaussian integer β if

a) $\alpha = 2 - i, \beta = 5 + 5i$.
b) $\alpha = 1 - i, \beta = 8$.
c) $\alpha = 5, \beta = 2 + 3i$.
d) $\alpha = 3 + 2i, \beta = 26$.

4. Determine whether the Gaussian integer α divides the Gaussian integer β, where

a) $\alpha = 3, \beta = 4 + 7i$.
b) $\alpha = 2 + i, \beta = 15$.
c) $\alpha = 5 + 3i, \beta = 30 + 6i$.
d) $\alpha = 11 + 4i, \beta = 274$.

5. Give a formula for all Gaussian integers divisible by $4 + 3i$ and display the set of all such Gaussian integers in the plane.

6. Give a formula for all Gaussian integers divisible by $4 - i$ and display the set of all such Gaussian integers in the plane.

7. Show that if α, β, and γ are Gaussian integers and $\alpha \mid \beta$ and $\beta \mid \gamma$, then $\alpha \mid \gamma$.

8. Show that if α, β, γ, μ, and ν are Gaussian integers and $\gamma \mid \alpha$ and $\gamma \mid \beta$, then $\gamma \mid (\mu\alpha + \nu\beta)$.

9. Show that if ϵ is a unit for the Gaussian integers, then $\epsilon^5 = \epsilon$.

10. Find all Gaussian integers $\alpha = a + bi$ such that $\overline{\alpha} = a - bi$, the conjugate of α, is an associate of α.

11. Show that the Gaussian integers α and β are associates if $\alpha \mid \beta$ and $\beta \mid \alpha$.

12. Show that if α and β are Gaussian integers and $\alpha \mid \beta$, then $N(\alpha) \mid N(\beta)$.

13. Suppose that $N(\alpha) \mid N(\beta)$, where α and β are Gaussian integers. Does it necessarily follow that $\alpha \mid \beta$? Supply either a proof or a counterexample.

14. Show that if α divides β, where α and β are Gaussian integers, then $\overline{\alpha}$ divides $\overline{\beta}$.

15. Show that if $\alpha = a + bi$ is a nonzero Gaussian integer, then α has exactly one associate $c + di$ (including α itself), where $c > 0$ and $d \geq 0$.

16. For each pair of values for α and β, find the quotient γ and the remainder ρ when α is divided by β computed following the construction in the proof of Theorem 14.6, and verify that $N(\rho) < N(\beta)$.

a) $\alpha = 14 + 17i, \beta = 2 + 3i$
b) $\alpha = 7 - 19i, \beta = 3 - 4i$
c) $\alpha = 33, \beta = 5 + i$

17. For each pair of values for α and β, find the quotient γ and the remainder ρ when α is divided by β computed following the construction in the proof of Theorem 14.6, and verify that $N(\rho) < N(\beta)$.

a) $\alpha = 24 - 9i, \beta = 3 + 3i$
b) $\alpha = 18 + 15i, \beta = 3 + 4i$
c) $\alpha = 87i, \beta = 11 - 2i$

18. For each pair of values for α and β in Exercise 16, find a pair of Gaussian integers γ and ρ such that $\alpha = \beta\gamma + \rho$ and $N(\rho) < N(\beta)$ different from that computed following the construction in Theorem 14.6.

19. For each pair of values for α and β in Exercise 17, find a pair of Gaussian integers γ and ρ such that $\alpha = \beta\gamma + \rho$ and $N(\rho) < N(\beta)$ different from that computed following the construction in Theorem 14.6.

20. Show that for every pair of Gaussian integers α and β with $\beta \neq 0$ and $\beta \nmid \alpha$, there are at least two different pairs of Gaussian integers γ and ρ such that $\alpha = \beta\gamma + \rho$ and $N(\rho) < N(\beta)$.

* **21.** Determine all possible values for the number of pairs of Gaussian integers γ and ρ such that $\alpha = \beta\gamma + \rho$ and $N(\rho) < N(\beta)$ when α and β are Gaussian integers and $\beta \neq 0$. (*Hint:* Analyze this geometrically by looking at the position of α/β in the square containing it and with four lattice points as its corners.)

22. Show that if a number of the form $r + si$, where r and s are rational numbers, is an algebraic integer, then r and s are integers.

23. Show that $1 + i$ divides a Gaussian integer $a + ib$ if and only if a and b are both even or both odd.

24. Show that if π is a Gaussian prime, then $N(\pi) = 2$ or $N(\pi) \equiv 1 \pmod 4$.

25. Find all Gaussian primes of the form $\alpha^2 + 1$, where α is a Gaussian integer.

26. Show that if $a + bi$ is a Gaussian prime, then $b + ai$ is also a Gaussian prime.

27. Show that the rational prime 7 is also a Gaussian prime by adapting the argument given in Example 14.6 that shows 3 is a Gaussian prime.

28. Show that every rational prime p of the form $4k + 3$ is also a Gaussian prime.

29. Suppose that α is a nonzero Gaussian integer which is neither a unit nor a prime. Show that a Gaussian integer β exists such that $\beta \mid \alpha$ and $1 < N(\beta) \leq \sqrt{N(\alpha)}$.

30. Explain how to adapt the sieve of Eratosthenes to find all the Gaussian primes with norm less than a specified limit.

31. Find all the Gaussian primes with norm less than 100.

32. Display all the Gaussian primes with norm less than 200 as lattice points in the plane.

We can define the notion of congruence for Gaussian integers. Suppose that α, β, and γ are Gaussian integers and that $\gamma \neq 0$. We say that α is *congruent* to β modulo γ and we write $\alpha \equiv \beta \pmod \gamma$ if $\gamma \mid (\alpha - \beta)$.

33. Suppose that μ is a nonzero Gaussian integer. Show that each of the following properties holds.

a) If α is a Gaussian integer, then $\alpha \equiv \alpha \pmod \mu$.

b) If $\alpha \equiv \beta \pmod \mu$, then $\beta \equiv \alpha \pmod \mu$.

c) If $\alpha \equiv \beta \pmod \mu$ and $\beta \equiv \gamma \pmod \mu$, then $\alpha \equiv \gamma \pmod \mu$.

34. Suppose that $\alpha \equiv \beta \pmod \mu$ and $\gamma \equiv \delta \pmod \mu$, where α, β, γ, δ, and μ are Gaussian integers and $\mu \neq 0$. Show that each of these properties holds.

a) $\alpha + \gamma \equiv \beta + \delta \pmod \mu$

b) $\alpha - \gamma \equiv \beta - \delta \pmod \mu$

c) $\alpha\gamma \equiv \beta\delta \pmod \mu$

35. Show that two Gaussian integers $\alpha = a_1 + ib_1$ and $\beta = a_2 + ib_2$ can multiplied using only three multiplications of rational integers, rather than the four in the equation shown

in the text, together with five additions and subtractions. (*Hint:* One way to do this uses the product $(a_1 + b_1)(a_2 + b_2)$. A second way uses the product $b_2(a_1 + b_1)$.)

36. When a and b are real numbers, let $\{a + bi\} = \{a\} + \{b\}i$, where $\{x\}$ is the closest integer to the real number x, rounding up in the case of a tie. Show that if z is a complex number, no Gaussian integer is closer to z than $\{z\}$ and $N(z - \{z\}) \leq 1/2$.

Let k be a nonnegative integer. The *Gaussian Fibonacci number* G_k is defined in terms of the Fibonacci numbers with $G_k = f_k + if_{k+1}$. Exercises 37–39 involve Gaussian Fibonacci numbers.

37. a) List the terms of the Gaussian Fibonacci sequence for $k = 0, 1, 2, 3, 4, 5$. (Recall that $f_0 = 0$.)

b) Show that $G_k = G_{k-1} + G_{k-2}$ for $k = 2, 3, \ldots$.

38. Show that $N(G_k) = f_{2k+1}$ for all nonnegative integers k.

39. Show that $G_{n+2}G_{n+1} - G_{n+3}G_n = (-1)^n(2 + i)$, whenever n is a positive integer.

40. Show that every Gaussian integer can be written in the form $a_n(-1 + i)^n + a_{n-1}(-1 + i)^{n-1} + \cdots + a_1(-1 + i) + a_0$, where $a_j = 0$ or 1 for $j = 0, 1, \ldots, n - 1, n$.

41. Show that if α is a number of the form $r + si$, where r and s are rational numbers and α is a root of a monic quadratic polynomial with integer coefficients, then α is a Gaussian integer.

42. What can you conclude if $\pi = a + bi$ is a Gaussian prime and one of the Gaussian integers $(a + 1) + bi$, $(a - 1) + bi$, $a + (b + 1)i$, and $a + (b - 1)i$ is also a Gaussian prime?

43. Show that if $\pi_1 = a - 1 + bi$, $\pi_2 = a + 1 + bi$, $\pi_3 = a + (b - 1)i$, and $\pi_4 = a + (b + 1)i$ are all Gaussian primes and $|a| + |b| > 5$, then 5 divides both a and b and neither a nor b is zero.

44. Describe the block of Gaussian integers containing no Gaussian primes that can be constructed by first forming the product of all Gaussian integers $a + bi$ with a and b rational integers, $0 \leq a \leq m$, and $0 \leq b \leq n$.

45. Find all Gaussian integers α, β, and γ such that $\alpha\beta\gamma = \alpha + \beta + \gamma = 1$.

46. Show that if π is a Gaussian prime with $N(\pi) \neq 2$, then exactly one of the associates of π is congruent to either 1 or $3 + 2i$ modulo 4.

14.1 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica*, or programs you have written, carry out the following computations and explorations.

1. Find all pairs of Gaussian integers γ and ρ such that $180 - 181i = (12 + 13i)\gamma + \rho$ and $N(\rho) < N(12 + 13i)$.

2. Use a version of the sieve of Eratosthenes to find all Gaussian primes with norm less than 1000.

3. Find as many different pairs of Gaussian primes that differ by 2 as you can.