The fundamental theorem of arithmetic can be used to prove the following result, which relates the famous Riemann zeta function to the prime numbers.

Theorem 3.19. If s is a real number with $s > 1$, then

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Not surprisingly, we will not prove Theorem 3.19 because its proof depends on results from analysis. We note here that the proof uses the fundamental theorem of arithmetic to show that the term $1/n^s$, where n is a positive integer, appears exactly once when the terms of the product on the right-hand side are expanded. To see this, we use the fact that

$$\frac{1}{1 - p_j^{-s}} = \sum_{k=0}^{\infty} \frac{1}{p_j^{k_s}}$$

and then we multiply these sums together, obtaining the term

$$\frac{1}{p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}}$$

when the denominator is the prime-power factorization of n exactly once. The details of the proof can be found in [HaWr79].

3.5 Exercises

1. Find the prime factorizations of each of the following integers.

   a) 36 e) 222 i) 5040
   b) 39 f) 256 j) 8000
   c) 100 g) 515 k) 9555
   d) 289 h) 989 l) 9999

2. Find the prime factorization of 111,111.
3. Find the prime factorization of 4,849,845.
4. Find all of the prime factors of each of the following integers.

   a) 100,000 b) 10,500,000 c) 10! d) $\binom{30}{10}$

5. Find all of the prime factors of each of the following integers.

   a) 196,608 b) 7,290,000 c) 20! d) $\binom{50}{25}$

6. Show that all of the powers in the prime-power factorization of an integer n are even if and only if n is a perfect square.
7. Which positive integers have exactly three positive divisors? Which have exactly four positive divisors?

8. Show that every positive integer can be written as the product of possibly a square and a square-free integer. A *square-free integer* is an integer that is not divisible by any perfect squares other than 1.

9. An integer n is called *powerful* if, whenever a prime p divides n, p^2 divides n. Show that every powerful number can be written as the product of a perfect square and a perfect cube.

10. Show that if a and b are positive integers and $a^3 \mid b^2$, then $a \mid b$.

Let p be a prime and n a positive integer. If $p^a \mid n$, but $p^{a+1} \nmid n$, we say that p^a *exactly divides* n, and we write $p^a \,||\, n$.

11. Show that if $p^a \,||\, m$ and $p^b \,||\, n$, then $p^{a+b} \,||\, mn$.

12. Show that if $p^a \,||\, m$, then $p^{ka} \,||\, m^k$.

13. Show that if $p^a \,||\, m$ and $p^b \,||\, n$ with $a \neq b$, then $p^{\min(a,b)} \,||\, (m+n)$.

14. Let n be a positive integer. Show that the power of the prime p occurring in the prime-power factorization of $n!$ is

$$[n/p] + [n/p^2] + [n/p^3] + \cdots.$$

15. Use Exercise 14 to find the prime-power factorization of 20!.

16. How many zeros are there at the end of 1000! in decimal notation? How many in base 8 notation?

17. Find all positive integers n such that $n!$ ends with exactly 74 zeros in decimal notation.

18. Show that if n is a positive integer, it is impossible for $n!$ to end with exactly 153, 154, or 155 zeros when it is written in decimal notation.

Let $\alpha = a + b\sqrt{-5}$, where a and b are integers. Define the *norm* of α, denoted by $N(\alpha)$, as $N(\alpha) = a^2 + 5b^2$.

19. Show that if $\alpha = a + b\sqrt{-5}$ and $\beta = c + d\sqrt{-5}$, where a, b, c, and d are integers, then $N(\alpha\beta) = N(\alpha)N(\beta)$.

20. A number of the form $a + b\sqrt{-5}$ is *prime* if it cannot be written as the product of numbers α and β, where neither α nor β equals ± 1. Show that the number 2 is a prime number of the form $a + b\sqrt{-5}$. (*Hint:* Start with $N(2) = N(\alpha\beta)$, and use Exercise 19.)

21. Use an argument similar to that in Exercise 20 to show that 3 is a prime number of the form $a + b\sqrt{-5}$.

22. Use arguments similar to that in Exercise 20 to show that both $1 \pm \sqrt{-5}$ are prime numbers of the form $a + b\sqrt{-5}$.

23. Find two different factorizations of the number 21 into primes of the form $a + b\sqrt{-5}$, where a and b are integers.

* **24.** Show that the set of all numbers of the form $a + b\sqrt{-6}$, where a and b are integers, does not enjoy the property of unique factorization.

The next four exercises present another example of a system where unique factorization into primes fails. Let H be the set of all positive integers of the form $4k + 1$, where k is a nonnegative integer.

25. Show that the product of two elements of H is also in H.

26. An element $h \neq 1$ in H is called a *Hilbert prime* (named after famous German mathematician *David Hilbert*) if the only way it can be written as the product of two integers in H is $h = h \cdot 1 = 1 \cdot h$. Find the 20 smallest Hilbert primes.

27. Show that every element of H can be factored into Hilbert primes.

28. Show that factorization of elements of H into Hilbert primes is not necessarily unique, by finding two different factorizations of 693 into Hilbert primes.

29. Which positive integers n are divisible by all integers not exceeding $\sqrt{n}$?

30. Find the least common multiple of each of the following pairs of integers.

a) 8, 12
b) 14, 15
c) 28, 35
d) 111, 303
e) 256, 5040
f) 343, 999

31. Find the least common multiple of each of the following pairs of integers.

a) 7, 11
b) 12, 18
c) 25, 30
d) 101, 333
e) 1331, 5005
f) 5040, 7700

32. Find the greatest common divisor and least common multiple of the following pairs of integers.

a) $2 \cdot 3^2 5^3$, $2^2 3^3 7^2$
b) $2 \cdot 3 \cdot 5 \cdot 7$, $7 \cdot 11 \cdot 13$
c) $2^8 3^6 5^4 11^{13}$, $2 \cdot 3 \cdot 5 \cdot 11 \cdot 13$
d) $41^{101} 47^{43} 103^{1001}$, $41^{11} 43^{47} 83^{111}$

DAVID HILBERT (1862–1943), born in Königsberg, the city famous in mathematics for its seven bridges, was the son of a judge. During his tenure at Göttingen University, from 1892 to 1930, Hilbert made many fundamental contributions to a wide range of mathematical subjects. He almost always worked on one area of mathematics at a time, making important contributions, then moving to a new mathematical subject. Some areas in which Hilbert worked are the calculus of variations, geometry, algebra, number theory, logic, and mathematical physics. Besides his many outstanding original contributions, Hilbert is remembered for his famous list of 23 difficult problems. He described these problems at the 1900 International Congress of Mathematicians, as a challenge to mathematicians at the birth of the twentieth century. Since that time, they have spurred a tremendous amount and variety of research. Although many of these problems have now been solved, several remain open, including the Riemann hypothesis, which is part of Problem 8 on Hilbert's list. Hilbert was also the author of several important textbooks in number theory and geometry.

33. Find the greatest common divisor and least common multiple of the following pairs of integers.

a) $2^2 3^3 5^5 7^7$, $2^7 3^5 5^3 7^2$

b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$, $17 \cdot 19 \cdot 23 \cdot 29$

c) $2^3 5^7 11^{13}$, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$

d) $47^{11} 79^{111} 101^{1001}$, $41^{11} 83^{111} 101^{1000}$

34. Show that every common multiple of the positive integers a and b is divisible by the least common multiple of a and b.

35. Periodical cicadas are insects with very long larval periods and brief adult lives. For each species of periodical cicada with a larval period of 17 years, there is a similar species with a larval period of 13 years. If both the 17-year and 13-year species emerged in a particular location in 1900, when will they next both emerge in that location?

36. Which pairs of integers a and b have greatest common divisor 18 and least common multiple 540?

37. Show that if a and b are positive integers, then $(a, b) \mid [a, b]$. When does $(a, b) = [a, b]$?

38. Show that if a and b are positive integers, then there are divisors c of a and d of b with $(c, d) = 1$ and $cd = [a, b]$.

☞ **39.** Show that if a, b, and c are integers, then $[a, b] \mid c$ if and only if $a \mid c$ and $b \mid c$.

☞ **40.** Use Lemma 3.4 to show that if p is a prime and a is an integer with $p \mid a^2$, then $p \mid a$.

☞ **41.** Show that if p is a prime, a is an integer, and n is a positive integer such that $p \mid a^n$, then $p \mid a$.

42. Show that if a, b, and c are integers with $c \mid ab$, then $c \mid (a, c)(b, c)$.

43. a) Show that if a and b are positive integers with $(a, b) = 1$, then $(a^n, b^n) = 1$ for all positive integers n.

b) Use part (a) to prove that if a and b are integers such that $a^n \mid b^n$, where n is a positive integer, then $a \mid b$.

44. Show that $\sqrt[3]{5}$ is irrational:

a) by an argument similar to that given in Example 3.20;

b) using Theorem 3.18.

45. Show that $\sqrt{2} + \sqrt{3}$ is irrational.

46. Show that $\log_2 3$ is irrational.

47. Show that $\log_p b$ is irrational, where p is a prime and b is a positive integer that is not the second or higher power of p.

* **48.** Let n be a positive integer greater than 1. Show that $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ is not an integer.

49. Show that if a and b are positive integers, then $(a, b) = (a + b, [a, b])$.

50. Find the two positive integers with sum 798 and least common multiple 10,780. (*Hint:* Use Exercise 49.)

51. Show that if a, b, and c are positive integers, then $([a, b], c) = [(a, c), (b, c)]$ and $[(a, b), c] = ([a, c], [b, c])$.

The *least common multiple* of the integers $a_1, a_2, \ldots, a_n$, which are not all zero, is the smallest positive integer that is divisible by all the integers $a_1, a_2, \ldots, a_n$; it is denoted by $[a_1, a_2, \ldots, a_n]$.

52. Find $[6, 10, 15]$ and $[7, 11, 13]$.

53. Show that $[a_1, a_2, \ldots, a_{n-1}, a_n] = [[a_1, a_2, \ldots, a_{n-1}], a_n]$.

54. Let n be a positive integer. How many pairs of positive integers satisfy $[a, b] = n$? (*Hint:* Consider the prime factorization of n.)

55. a) Show that if a, b, and c are positive integers, then

$$\max(a, b, c) = a + b + c - \min(a, b) - \min(a, c) - \min(b, c) + \min(a, b, c).$$

b) Use part (a) to show that

$$[a, b, c] = \frac{abc(a, b, c)}{(a, b)(a, c)(b, c)}.$$

56. Generalize Exercise 55 to find a formula relating $(a_1, a_2, \ldots, a_n)$ and $[a_1, a_2, \ldots, a_n]$, where $a_1, a_2, \ldots, a_n$ are positive integers.

57. Show that if a, b, and c are positive integers, then $(a, b, c)[ab, ac, bc] = abc$.

58. Show that if a, b, and c are positive integers, then $[a, b, c](ab, ac, bc) = abc$.

59. Show that if a, b, and c are positive integers, then $([a, b], [a, c], [b, c]) = [(a, b), (a, c), (b, c)]$.

60. Prove that there are infinitely many primes of the form $6k + 5$, where k is a positive integer.

* **61.** Show that if a and b are positive integers, then the arithmetic progression a, $a + b$, $a + 2b, \ldots$, contains an arbitrary number of consecutive composite terms.

62. Find the prime factorizations of each of the following integers.

a) $10^6 - 1$ d) $2^{24} - 1$
b) $10^8 - 1$ e) $2^{30} - 1$
c) $2^{15} - 1$ f) $2^{36} - 1$

63. A discount store sells a camera at a price less than its usual retail price of \$99 but more than \$1. If they sell \$8137 worth of this camera and the discounted dollar price is an integer, how many cameras did they sell?

64. A publishing company sells \$375,961 worth of a particular book. How many copies of the book did they sell if their price is an exact dollar amount which is more than \$1?

65. If a store sells \$139,499 worth of electronic organizers at a sale price which is an exact dollar amount less than \$300 and more than \$1, how many electronic organizers did they sell?

66. Show that if a and b are positive integers, then $a^2 \mid b^2$ implies that $a \mid b$.

67. Show that if a, b, and c are positive integers with $(a, b) = 1$ and $ab = c^n$, then there are positive integers d and e such that $a = d^n$ and $b = e^n$.

☞ **68.** Show that if $a_1, a_2, \ldots, a_n$ are pairwise relatively prime integers, then $[a_1, a_2, \ldots, a_n] = a_1 a_2 \cdots a_n$.

69. Show that among any set of $n + 1$ positive integers not exceeding $2n$, there is an integer that divides a different integer in the set.

70. Show that $(m + n)!/m!n!$ is an integer whenever m and n are positive integers.

*** 71.** Find all solutions of the equation $m^n = n^m$, where m and n are integers.

72. Let $p_1, p_2, \ldots, p_n$ be the first n primes and let m be an integer with $1 < m < n$. Let Q be the product of a set of m primes in the list and let R be the product of the remaining primes. Show that $Q + R$ is not divisible by any primes in the list, and hence must have a prime factor not in the list. Conclude that there are infinitely many primes.

73. This exercise presents another proof that there are infinitely many primes. Assume that there are exactly r primes $p_1, p_2, \ldots, p_r$. Let $Q_k = \left(\prod_{j=1}^{r} p_j\right)/p_k$ for $k = 1, 2, \ldots, r$. Let $S = \sum_{j=1}^{r} Q_j$. Show that S must have a prime factor not among the r primes listed. Conclude that there are infinitely many primes. (This proof was published by G. Métrod in 1917.)

74. Show that if p is prime and $1 \leq k < p$, then the binomial coefficient $\binom{p}{k}$ is divisible by p.

75. Prove that in the prime factorization of $n!$, where n is an integer with $n > 1$, there is at least one prime factor with 1 as its exponent. (*Hint:* Use Bertrand's postulate.)

Exercises 76 and 77 outline two additional proofs that there are infinitely many primes.

76. Suppose that $p_1, \ldots, p_j$ are the first j primes, listed in increasing order. Denote by $N(x)$ the number of integers n not exceeding the integer x that are not divisible by any prime exceeding p_j.

a) Show that every integer n not divisible by any prime exceeding p_j can be written in the form $n = r^2 s$, where s is square-free.

b) Show there are only 2^j possible values of s in part (a) by looking at the prime factorization of such an integer n, which is a product of terms $p_k^{e_k}$, where $0 \leq k \leq j$ and e_k is 0 or 1.

c) Show that if $n \leq x$, then $r \leq \sqrt{n} \leq \sqrt{x}$, where r is in part (a). Conclude that there are no more than $\sqrt{x}$ different values possible for r. Conclude that $N(x) \leq 2^j \sqrt{x}$.

d) Show that if the number of primes is finite and p_j is the largest prime, then $N(x) = x$ for all integers x.

e) Show from parts (c) and (d) that $x \leq 2^j \sqrt{x}$, so that $x \leq 2^{2j}$ for all x, leading to a contradiction. Conclude that there must be infinitely many primes.

*** 77.** This exercise develops a proof that there are infinitely many primes based on the fundamental theorem of arithmetic published by A. Auric in 1915. Assume that there are exactly r primes, $p_1 < p_2 < \cdots < p_r$. Suppose that n is a positive integer and let $Q = p_r^n$.

a) Show that an integer m with $1 \leq m \leq Q$ can be written uniquely as $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, where $e_i \geq 0$ for $i = 1, 2, \ldots, r$. Furthermore, show that for the integer m with this factorization, $p_1^{e_1} \leq m \leq Q = p_r^n$.

b) Let $C = (\log p_r)/(\log p_1)$. Show that $e_i \leq nC$ for $i = 1, 2, \ldots, r$ and that Q does not exceed the number of r-tuples $(e_1, e_2, \ldots, e_r)$ of exponents in the prime-power factorizations of integers m with $1 \leq m \leq Q$.