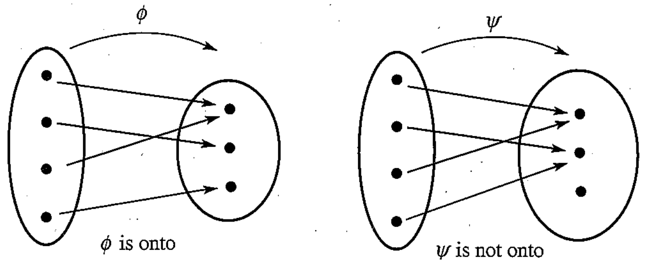

Figure 0.8

Theorem 0.7 **Properties of Functions**

Given functions $\alpha: A \to B$, $\beta: B \to C$, and $\gamma: C \to D$, then

1. *$\gamma(\beta\alpha) = (\gamma\beta)\alpha$ (associativity).*
2. *If α and β are one-to-one, then $\beta\alpha$ is one-to-one.*
3. *If α and β are onto, then $\beta\alpha$ is onto.*
4. *If α is one-to-one and onto, then there is a function α^{-1} from B onto A such that $(\alpha^{-1}\alpha)(a) = a$ for all a in A and $(\alpha\alpha^{-1})(b) = b$ for all b in B.*

PROOF. We prove only part 1. The remaining parts are left as exercises (Exercise 53). Let $a \in A$. Then $(\gamma(\beta\alpha))(a) = \gamma((\beta\alpha)(a)) = \gamma(\beta(\alpha(a)))$. On the other hand, $((\gamma\beta)\alpha)(a) = (\gamma\beta)(\alpha(a)) = \gamma(\beta(\alpha(a)))$. So, $\gamma(\beta\alpha) = (\gamma\beta)\alpha$. ■■

EXAMPLE 18 Let **Z** denote the set of integers, **R** the set of real numbers, and **N** the set of nonnegative integers. The following table illustrates the properties of one-to-one and onto.

Domain	**Range**	**Rule**	**One-to-one**	**Onto**
Z	**Z**	$x \to x^3$	Yes	No
R	**R**	$x \to x^3$	Yes	Yes
Z	**N**	$x \to \lvert x \rvert$	No	Yes
Z	**Z**	$x \to x^2$	No	No

To verify that $x \to x^3$ is one-to-one in the first two cases, notice that if $x^3 = y^3$, we may take the cube roots of both sides of the equation to obtain $x = y$. Clearly, the mapping from **Z** to **Z** given by $x \to x^3$ is not onto, since 2 is the cube of no integer. However, $x \to x^3$ defines an onto function from **R** to **R**, since every real number is the cube of its

EXERCISES

If you really want something in this life, you have to work for it—Now quiet, they're about to announce the lottery numbers!

HOMER SIMPSON

1. For $n = 5, 8, 12, 20$, and 25, find all positive integers less than n and relatively prime to n.

2. Determine $\gcd(2^4 \cdot 3^2 \cdot 5 \cdot 7^2, 2 \cdot 3^3 \cdot 7 \cdot 11)$ and $\operatorname{lcm}(2^3 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7 \cdot 11)$.

3. Determine 51 mod 13, 342 mod 85, 62 mod 15, 10 mod 15, $(82 \cdot 73)$ mod 7, $(51 + 68)$ mod 7, $(35 \cdot 24)$ mod 11, and $(47 + 68)$ mod 11.

4. Find integers s and t such that $1 = 7 \cdot s + 11 \cdot t$. Show that s and t are not unique.

5. In Florida, the fourth and fifth digits from the end of a driver's license number give the year of birth. The last three digits for a male with birth month m and birth date b are represented by $40(m - 1) + b$. For females the digits are $40(m - 1) + b + 500$. Determine the dates of birth of people who have last five digits 42218 and 53953.

6. For driver's license numbers issued in New York prior to September of 1992, the three digits preceding the last two of the number of a male with birth month m and birth date b are represented by $63m + 2b$. For females the digits are $63m + 2b + 1$. Determine the dates of birth and sex(es) corresponding to the numbers 248 and 601.

7. Show that if a and b are positive integers, then $ab = \operatorname{lcm}(a, b) \cdot \gcd(a, b)$.

8. Suppose a and b are integers that divide the integer c. If a and b are relatively prime, show that ab divides c. Show, by example, that if a and b are not relatively prime, then ab need not divide c.

9. If a and b are integers and n is a positive integer, prove that $a \bmod n = b \bmod n$ if and only if n divides $a - b$.

10. Let $d = \gcd(a, b)$. If $a = da'$ and $b = db'$, show that $\gcd(a', b') = 1$.

11. Let n be a fixed positive integer greater than 1. If $a \bmod n = a'$ and $b \bmod n = b'$, prove that $(a + b) \bmod n = (a' + b') \bmod n$ and $(ab) \bmod n = (a'b') \bmod n$. (This exercise is referred to in Chapters 6, 8, and 15.)

12. Let a and b be positive integers and let $d = \gcd(a, b)$ and $m = \operatorname{lcm}(a, b)$. If t divides both a and b, prove that t divides d. If s is a multiple of both a and b, prove that s is a multiple of m.

13. Let n and a be positive integers and let $d = \gcd(a, n)$. Show that the

15. Let a, b, s, and t be integers. If $a \bmod st = b \bmod st$, show that $a \bmod s = b \bmod s$ and $a \bmod t = b \bmod t$. What condition on s and t is needed to make the converse true? (This exercise is referred to in Chapter 8.)

16. Use the Euclidean algorithm to find gcd(34, 126) and write it as a linear combination of 34 and 126.

17. Show that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$. (This exercise is referred to in Chapter 8.)

18. Let $p_1, p_2, \ldots, p_n$ be primes. Show that $p_1 p_2 \cdots p_n + 1$ is divisible by none of these primes.

19. Prove that there are infinitely many primes. (*Hint:* Use Exercise 18.)

20. For every positive integer n, prove that $1 + 2 + \cdots + n = n(n + 1)/2$.

21. For every positive integer n, prove that a set with exactly n elements has exactly 2^n subsets (counting the empty set and the entire set).

22. Prove that $2^n 3^{2n} - 1$ is always divisible by 17.

23. Prove that there is some positive integer n such that $n, n + 1, n + 2, \ldots, n + 200$ are all composite.

24. (Generalized Euclid's Lemma) If p is a prime and p divides $a_1 a_2 \cdots a_n$, prove that p divides a_i for some i.

25. Use the Generalized Euclid's Lemma (see Exercise 24) to establish the uniqueness portion of the Fundamental Theorem of Arithmetic.

26. What is the largest bet that cannot be made with chips worth \$7.00 and \$9.00? Verify that your answer is correct with both forms of induction.

27. Prove that the First Principle of Mathematical Induction is a consequence of the Well Ordering Principle.

28. The Fibonacci numbers are: 1, 1, 2, 3, 5, 8, 13, 21, 34, ... In general, the Fibonacci numbers are defined by $f_1 = 1$, $f_2 = 1$, and for $n \geq 3$, $f_n = f_{n-1} + f_{n-2}$. Prove that the nth Fibonacci number f_n satisfies $f_n < 2^n$.

29. In the cut "As" from *Songs in the Key of Life*, Stevie Wonder mentions the equation $8 \times 8 \times 8 \times 8 = 4$. Find all integers n for which this statement is true, modulo n.

30. Prove that for every integer n, $n^3 \bmod 6 = n \bmod 6$.

31. If it were 2:00 A.M. now, what time would it be 3736 hours from now?

32. Determine the check digit for a money order with identification number 7234541780.

33. Suppose that in one of the noncheck positions of a money order number, the digit 0 is substituted for the digit 9 or vice versa. Prove that this error will not be detected by the check digit. Prove that all other errors involving a single position are detected.