Next, we multiply each digit by the appropriate weight according to step (2) in the check-digit scheme for VINs, and we add as follows:

$$
\begin{aligned}
&8(1) + 7(7) + 6(4) + 5(8) + 4(7) + 3(5) + 2(4) + 10(3) + 9(2) + \\
&\qquad 8(8) + 7(4) + 6(1) + 5(0) + 4(0) + 3(3) + 2(0) \\
&= 8 + 49 + 24 + 40 + 28 + 15 + 8 + 30 + 18 + 64 + 28 + 6 + 0 + 0 + 9 + 0 \\
&= 327.
\end{aligned}
$$

For the VIN to be a valid number, this number must be congruent modulo 11 to the check digit 5. In other words, the difference between 327 and 5 must be divisible by 11. Unfortunately, when the difference $327 - 5 = 322$ is divided by 11, there is a remainder of 3. Thus, 327 is *not* congruent to 5 modulo 11, so the check digit is incorrect. This means that the VIN is not valid. You had better not buy that car!

PROBLEM SET 1.2

1. Consider the following long-division problem.

$$
\begin{array}{r}
44 \\
14\overline{)627} \\
\underline{56} \\
67 \\
\underline{56} \\
11
\end{array}
$$

a. Identify the divisor, dividend, quotient, and remainder.

b. Express the relationship among the divisor, dividend, quotient, and remainder using the division algorithm for whole numbers.

c. Is it true that $14 \mid 627$? Explain.

2. Consider the following long-division problem.

$$
\begin{array}{r}
87 \\
29\overline{)2523} \\
\underline{232} \\
203 \\
\underline{203} \\
0
\end{array}
$$

a. Identify the divisor, dividend, quotient, and remainder.

b. Express the relationship among the divisor, dividend, quotient, and remainder using the division algorithm for whole numbers.

c. Is it true that $29 \mid 2523$? Explain.

3. Decide if each of the following statements is true or false. Justify your answers.

a. $3 \mid 12$ **b.** $5 \mid 474$

c. $18 \mid 1116$ **d.** $31 \mid 1458$

4. Decide if each of the following statements is true or false. Justify your answers.

a. $6 \mid 19$

b. $9 \mid 585$

c. $32 \mid 807$

d. $46 \mid 4370$

Problems 5 and 6

Use a calculator and the division algorithm for integers to find the quotient and remainder.

5. a. divisor = 12, dividend = 447

b. divisor = 53, dividend = −887

c. divisor = 91, dividend = 5938

6. a. divisor = 18, dividend = −1727

b. divisor = 164, dividend = 1317

c. divisor = 33, dividend = 8721

7. When any integer is divided by 3, there will be a remainder of 0, 1, or 2. For each integer, determine the remainder after a division by 3. Fill in the following table as was done in Table 1.5 for division by 7; that is, list in each row those integers for which the remainder is 0, 1, or 2.

Integer	Remainder
	0
	1
	2

8. When any integer is divided by 4, there will be a remainder of 0, 1, 2, or 3. For each integer, determine the remainder after a division by 4. Fill in the following table as was done in Table 1.5 for division by 7; that is, list in each row those integers for which the remainder is 0, 1, 2, or 3.

Integer	Remainder
	0
	1
	2
	3

Problems 9 and 10

Use the definition of congruence modulo m to verify each of the congruencies.

9. **a.** $39 \equiv 0 \bmod 3$ **b.** $29 \equiv 4 \bmod 5$
c. $72 \equiv 18 \bmod 6$ **d.** $81 \equiv 21 \bmod 4$

10. **a.** $105 \equiv 42 \bmod 3$ **b.** $55 \equiv 13 \bmod 6$
c. $107 \equiv 71 \bmod 9$ **d.** $97 \equiv 25 \bmod 3$

Problems 11 and 12

Use the definition of congruence modulo m to determine if each of the statements is true or false. Justify your answer.

11. **a.** $-55 \equiv 0 \bmod 4$ **b.** $64 \equiv -5 \bmod 7$
c. $87 \equiv 6 \bmod 13$ **d.** $-24 \equiv -4 \bmod 10$

12. **a.** $-103 \equiv 98 \bmod 2$ **b.** $59 \equiv 67 \bmod 8$
c. $95 \equiv -49 \bmod 15$ **d.** $-38 \equiv -6 \bmod 4$

13. Use arithmetic property (4) of congruence modulo m to compute each of the following sums modulo 6 in two ways. First, evaluate congruence modulo 6 before adding, and second, evaluate congruence modulo 6 after adding.
a. $15 + 41$ **b.** $25 + 58$ **c.** $76 + 14$

14. Use arithmetic property (4) of congruence modulo m to compute each of the following sums modulo 4 in two ways. First, evaluate congruence modulo 4 before adding, and second, evaluate congruence modulo 4 after adding.
a. $17 + 11$ **b.** $55 + 35$ **c.** $44 + 21$

15. Use arithmetic property (5) of congruence modulo m to compute each of the following products modulo 7 in two ways. First, evaluate congruence modulo 7 before multiplying, and second, evaluate congruence modulo 7 after multiplying.
a. 17×11 **b.** 55×35 **c.** 44×29

16. Use arithmetic property (5) of congruence modulo m to compute each of the following products modulo 9 in two ways. First, evaluate congruence modulo 9 before multiplying, and second, evaluate congruence modulo 9 after multiplying.
a. 23×11 **b.** 63×35 **c.** 48×26

17. **a.** Find the smallest whole-number value of b in $52 \times 28 \equiv b \bmod 5$ to make the congruence true.
b. Find the smallest whole-number value of c in $71 \times c \equiv 4 \bmod 8$ to make the congruence true.

18. **a.** Find the smallest whole-number value of b in $39 \times 73 \equiv b \bmod 8$ to make the congruence true.
b. Find the smallest whole-number value of c in $29 \times c \equiv 2 \bmod 5$ to make the congruence true.

19. Evaluate each of the following powers.
a. $3^{200} \bmod 8$ **b.** $2^{311} \bmod 9$ **c.** $5^{142} \bmod 9$

20. Evaluate each of the following powers.
a. $4^{300} \bmod 3$ **b.** $3^{302} \bmod 5$ **c.** $3^{191} \bmod 7$

Problems 21 and 22

Next to the day, the week is the most significant block of time in modern life. A week is a cycle of seven days. Determining the day of the week at some point in the future is a modular arithmetic problem. For example, because $4 \equiv 11 \bmod 7$, we know that if January 4 is a Monday, then January 11 will also be a Monday.

21. **a.** If today is Friday, use congruence modulo 7 to determine what day of the week it will be in 48 days.
b. If May 14, 2003 was a Wednesday, use congruence modulo 7 to determine the day of the week on which August 3, 2003, fell.

22. **a.** If today is Monday, use congruence modulo 7 to determine what day of the week it will be in 61 days.
b. If March 1, 2004 was a Monday, use congruence modulo 7 to determine the day of the week on which January 15, 2006 fell.

Problems 23 through 26

A leap year has an extra day in February, making the year 366 days long. How can you figure out which years are leap years? If we let L be the year, then L is a leap year when $L \equiv 0 \bmod 4$ unless $L \equiv 0 \bmod 100$. There is an exception to the rule. If $L \equiv 0 \bmod 400$, then L is a leap year.

23. Determine if the year is a leap year.
a. 1980 **b.** 2023 **c.** 2008
d. 2000 **e.** 1800

24. Determine if the year is a leap year.

a. 1941 **b.** 3000 **c.** 2036
d. 2400 **e.** 2324

25. The year 2092 will be a leap year. If someone is born on February 29, 2092, and decides to celebrate birthdays only on February 29, how many birthdays will he or she have celebrated by the year 2150?

26. The year 2000 was a leap year. If someone was born on February 29, 2000, and decides to celebrate birthdays only on February 29, how many birthdays will he or she have celebrated by the year 2070?

27. A doctor's office uses a five-digit identification code for filing and retrieving patient records so that the fifth digit is the check digit. The code will use a mod 7 check-digit scheme; that is, the check digit is congruent to $d_1d_2d_3d_4$ mod 7.

a. What digits are possible as check digits?

b. Find the check digit for the identification code 3964.

c. Find the missing digit in the code 41?73.

28. A teacher created a 6-digit student identification number so that the sixth digit is the check digit. The code will use a mod 8 check-digit scheme; that is, the check digit is congruent to $d_1d_2d_3d_4d_5$ mod 8.

a. What digits are possible as check digits?

b. Find the check digit for the identification code 52891.

c. Find the missing digit in the code 3017?2.

Problems 29 and 30

Suppose you are given a five-digit identification number that you know uses a modular check-digit scheme in which the check digit is the remainder when the number represented by the first four digits is divided by m. You do not know the modulus, but you know the fifth digit is the check digit.

29. If your identification number is 24396, what are the possible values for m?

30. If your identification number is 58237, what are the possible values for m?

Problems 31 and 32

Use the process of casting out nines to answer the following.

31. Suppose a U.S. Post Office money order is identified by the 10-digit number 3872219457. What mod 9 check digit should be in the 11th position?

32. Suppose a U.S. Post Office money order is identified by the 10-digit number 1072385148. What mod 9 check digit should be in the 11th position?

33. a. The country digit is missing from the Euro banknote with serial number 83654297554. Use Table 1.6 to determine the possible countries of origin.

b. The check digit is missing for the Euro banknote with alphanumeric serial number P2974653389. Use Table 1.6 and determine the check digit required to make the sum of all 12 digits divisible by 9.

34. a. The country digit is missing from the Euro banknote with serial number 35529768044. Use Table 1.6 to determine the possible countries of origin.

b. The check digit is missing for the Euro banknote with alphanumeric serial number T1104873647. Use Table 1.6 and determine the check digit required to make the sum of all 12 digits divisible by 9.

35. a. Is an airline ticket with number 01634287759320 a valid ticket?

b. Find the mod 7 check digit for the airline ticket number 0161466117765.

36. a. Is an airline ticket with number 01282976502243 a valid ticket?

b. Find the mod 7 check digit for the airline ticket number 0120117309603.

Problems 37 and 38

Tracking numbers are used by the United Parcel Service (UPS) to track packages as they move through the system. The number may be used by the consumer to verify delivery or to locate a package en route to its destination. The tracking number is 18 characters long and begins with the combination 1Z, which is not used to calculate the check digit. The check digit is the 18th digit and can be found using a mod 7 check-digit scheme on the number represented by the digits in positions 3 through 17.

37. a. Determine if 1Z5915806860472484 is a valid UPS tracking number.

b. Find the check digit for the partial UPS tracking number 1Z433698652447694.

38. a. Determine if 1Z7346528967467741 is a valid UPS tracking number.

b. Find the check digit for the partial UPS tracking number 1Z983211056358736.

39. Each of the following vehicle identification numbers is missing a digit. Find the missing digit.

a. 19UY?3255XL001438

b. 1G3?R64H824236950

40. Each of the following vehicle identification numbers is missing a digit. Find the missing digit.

a. 1?3NF52E3XC360981

b. 1G8JW52R3Y?624765

Problems 41 and 42

Another alphanumeric code was developed in the 1970s. It is known by names such as **Code 39** and **Code 3 of 9**. It is a variable-length code that has been used by the Department of Defense, in nonretail and industrial applications, in warehouse and inventory management, and in the pharmaceutical industry. The code uses the digits 0 through 9, the uppercase letters of the alphabet, and several symbols. A check digit is not required, but when a check digit is included, the code uses a mod 43 check-digit scheme on the sum of the character values and the check digit is the last character in the identification number. In order to calculate the check digit, each character must be assigned a value according to the following table. Notice that some punctuation symbols are significant in this coding system.

Character	Value	Character	Value	Character	Value	Character	Value
0	0	B	11	M	22	X	33
1	1	C	12	N	23	Y	34
2	2	D	13	O	24	Z	35
3	3	E	14	P	25	-	36
4	4	F	15	Q	26	.	37
5	5	G	16	R	27	space	38
6	6	H	17	S	28	$	39
7	7	I	18	T	29	/	40
8	8	J	19	U	30	+	41
9	9	K	20	V	31	%	42
A	10	L	21	W	32		

41. a. Assuming a check digit has been used, is 2A−482TWZ a valid Code 39 identification number?

b. For a Code 39 identification number SP245399MX65, find the check digit.

42. a. Assuming a check digit has been used, is DLA50084M4081A a valid Code 39 identification number?

b. For a Code 39 identification number T934RD%8Q, find the check digit.

Extended Problems

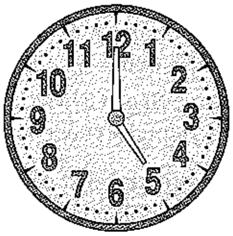
43. According to the historian E. T. Bell, Carl Friedrich Gauss "lives everywhere in mathematics." Modular arithmetic is only one of the many discoveries made by Gauss. Research the accomplishments of Gauss and summarize your findings in a report. In particular, be sure to investigate his work in the area of modular arithmetic.

44. In the definition of congruence modulo m, the values a, b, and m are integers with $m \geq 2$. Explain why neither 0 nor 1 may be used for m.

45. The Vehicle Identification Number (VIN) standards were created in 1977 and revised in 1983. The VIN uniquely identifies a vehicle. Each of the 17 alphanumeric characters has a meaning. For example, in a typical VIN, the first character identifies the country of origin (U.S. = 1, Canada = 2, Mexico = 3, Japan = J, etc.) The character in the second position often identifies the manufacturer (Audi = A, Dodge = B, Ford = F, etc.) The ninth digit is the check digit. The letters I and O are not valid in a VIN since they are easily mistaken for the numbers 1 and 0. What kind of car do you drive? Who is the manufacturer? Copy the VIN from your car or the car of someone you know. Go online and research the VIN for a specific manufacturer. Search keywords "vehicle identification number." For each character in the VIN, list the codes and meanings for this manufacturer. For your VIN, identify the digit in each position and describe all the information it provides. Verify that the check digit is correct and show your calculation.

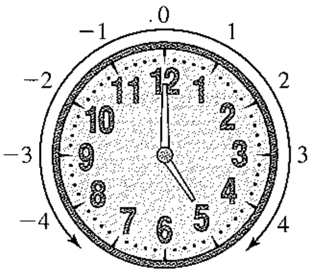
Problems 46 and 47

Clock arithmetic is arithmetic done on a clock rather than a number line. We are all most comfortable with a 12-hour clock, although we could create clocks with fewer hours or with more hours. First, consider a typical clock face with 12 numbers. We might ask the question, "If it is 5 o'clock now, what time will it be in 10 hours?"



Moving in a clockwise direction moves the hour hand 10 hours forward. When we add in the usual sense, $5 + 10 = 15$, but on a clock, we start counting over after we reach 12 o'clock, so the answer to the question, of course, is 3 o'clock. Notice that adding hours on a clock is a modular arithmetic problem using modulus 12, since $15 \equiv 3 \bmod 12$.

In performing clock arithmetic, we could think of wrapping the integer number line around and around the clock with 0 corresponding to 12. Each integer is congruent modulo 12 to one of the numbers from 0 through 11, so there are infinitely many integers associated with each clock number.



The integers associated with the number 3, for example, are . . . , −33, −21, −9, 3, 15, 27, ... Notice that the difference of any two integers is a multiple of 12, so each integer in this list is congruent to 3 modulo 12.

If we introduce a special notation, we can distinguish clock arithmetic from the usual arithmetic. When we added 5 and 10 using the 12-hour clock, we noted that $5 + 10 \equiv 3 \bmod 12$. Sometimes this is written $5 \oplus 10 = 3$ to indicate that we are doing clock arithmetic. Note that the modulus can change if we use a clock with a different number of hours, but we use the notation $\oplus$ with any clock.

Subtraction can also be defined for clock arithmetic. We could ask, "If it is 5 o'clock now, what time was it 10 hours ago?" We know that it would be 7 o'clock if we count backward from 5 using the 12-hour clock, since $5 - 10 \equiv 7 \bmod 12$. Using clock arithmetic notation and a 12-hour clock, we would write $5 \ominus 10 = 7$. We define subtraction on the 12-hour clock as follows: subtract whole numbers as usual, as in $9 \ominus 2 = 7$, but if the difference is less than 0, add 12. For example $3 \ominus 8 = -5 + 12 = 7$.

46. **a.** Use clock arithmetic to calculate each of the following using a 7-hour clock.

(i) $5 \oplus 6$

(ii) $4 \oplus 2$

(iii) $6 \ominus 2$

(iv) $1 \ominus 5$

b. Calculate each of the following using a 5-hour clock.

(i) $3 \oplus 4$

(ii) $1 \oplus 3$

(iii) $4 \ominus 3$

(iv) $1 \ominus 4$

c. Find two different clocks for which the integer 56 is 6 o'clock.

d. Find four different clocks for which the integer −19 is 1 o'clock.

47. We can think of multiplication as repeated addition, so we can define clock multiplication using clock addition. For example, $3 \otimes 4 = 4 \oplus 4 \oplus 4$.

a. Calculate $5 \otimes 3$ using a 6-hour clock.

b. Calculate $9 \otimes 2$ using a 14-hour clock.

c. Calculate $6 \otimes 6$ using an 8-hour clock.

d. Find all possible replacements for x to make the following true on a 7-hour clock: $3 \otimes x = 2$.

e. Find all possible replacements for x to make the following true on a 10-hour clock: $5 \otimes x = 0$.

f. Find all possible replacements for x to make the following true on an 8-hour clock: $7 \otimes x = 5$.

48. You can use the method of casting out nines to check your arithmetic by applying the following reasoning. If a is any whole number and a^* is the sum of the digits of a, then $a \equiv a^* \bmod 9$, as discussed in Example 1.14. If b is any whole number and b^* is the sum of the digits of b, then $b \equiv b^* \bmod 9$. Finally, if $c = a + b$ and c^* is the sum of the digits of c, then $c \equiv c^* \bmod 9$. When adding numbers, rather than add the numbers a second time to check our work, we can check our work by using the fact that if $a + b = c$, then $a^* + b^* \equiv c^* \bmod 9$ according to arithmetic property (4) of congruence modulo m. For example, if $a = 247{,}391$, $b = 87{,}654$, and $c = a + b$, then $c = 335{,}045$ and a^*, b^*, and c^* are defined as shown below:

	Sum of Digits
247,391	$a^* = 26$
+ 87,654	$b^* = 30$
335,045	$c^* = 20$

To check that the sum is correct, verify that $a^* + b^* \equiv c^*$:

$$a^* + b^* = 26 + 30 = 56 \equiv 2 \bmod 9$$
$$c^* = 20 \equiv 2 \bmod 9$$

Since $a^* + b^* \equiv 2 \bmod 9$ and $c^* \equiv 2 \bmod 9$, then $a^* + b^* \equiv c^*$.
Thus, the sum appears to be correct.

a. Use the method of casting out nines to check the following addition problem.

$$\begin{array}{r} 83{,}246 \\ +\ 7397 \\ \hline 90{,}643 \end{array}$$

b. Does verifying the congruence mod 9 by casting out nines guarantee that a sum has been calculated correctly? Explain and give an example.

c. This method can also be used to check multiplication by using the fact that if $a \times b = c$, then $(a^* \times b^*) \equiv c^* \bmod 9$. Use the method of casting out nines to check the following multiplication problem: $5678 \times 21{,}433 = 121{,}696{,}574$.

49. Cryptography is the science of encoding messages. One of the earliest systems for encoding messages was used by Julius Caesar and is known as the **Caesar cipher**. The Caesar cipher consists of replacing each letter in a message by the letter three places beyond it in alphabetical order. For example, suppose the message to be encoded is

SEND THE LEGION NORTH.

Under each letter of the message we write the letter three places further along in the alphabet as follows:

SEND THE LEGION NORTH
VHQG WKH OHJLRQ QRUWK.

Thus, the second line is the encoded message.

The Caesar cipher is an example of a **substitution cipher**, in which each letter of the original message is replaced by another. The Caesar cipher uses the **general system** of advancing the letter by adding a fixed number, namely 3, to its numerical equivalent using 26-hour clock arithmetic. Because knowing the number 3 tells you exactly how to encode and decode messages in the Caesar cipher, 3 is called the **key**. Encoding messages by adding a number in 26-hour clock arithmetic is called a **direct standard alphabet code**.

a. Encode the message LEAVE TUESDAY using a direct standard alphabet code and key 7.

b. Encode the message MAKE MY DAY using a direct standard alphabet code and key 14.

c. Decode the message WZNVPC WIGT using a direct standard alphabet code and key 11.

d. Decode the message CNM GUACW using a direct standard alphabet code and key 20.

50. The direct standard alphabet code relies on addition in 26-hour-clock arithmetic. Another substitution method, called **decimation**, relies on multiplication in 26-clock arithmetic. The number you multiply by, called the key, can be any number that has no factor in common with 26 such as 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, and 25. Suppose you select a key of 3. The letter A, which corresponds to 1, will be replaced by $3 \otimes 1 = 3$, which corresponds to C. Similarly B, which corresponds to 2, will be replaced by $3 \otimes 2 = 3 \oplus 3 = 6$, which corresponds to the letter F. Each subsequent replacement letter is obtained by adding another 3 in the 26-clock.

a. Encode or decode each of the following messages using decimation with the key 3.

(i) NEW YORK

(ii) GOW QOEH

b. Encode a message using decimation with 5 as the key.

c. Explain why the key used with decimation must not have factors in common with 26.