where $d_i = a_i - c_i$ for $i = 0, 1, \ldots, m$. Because the two representations for N are assumed different, we must have $d_i \neq 0$ for some value of i. Take k to be the smallest subscript for which $d_k \neq 0$. Then

$$0 = d_m b^m + \cdots + d_{k+1} b^{k+1} + d_k b^k$$

and so, after dividing by b^k,

$$d_k = -b(d_m b^{m-k-1} + \cdots + d_{k+1}).$$

This tells us that $b \mid d_k$. Now the inequalities $0 \leq a_k < b$ and $0 \leq c_k < b$ lead to $-b < a_k - c_k < b$, or $|d_k| < b$. The only way of reconciling the conditions $b \mid d_k$ and $|d_k| < b$ is to have $d_k = 0$, which is impossible. From this contradiction, we conclude that the representation of N is unique.

The essential feature in all of this is that the integer N is completely determined by the ordered array $a_m, a_{m-1}, \ldots, a_1, a_0$ of coefficients, with the powers of b and plus signs being superfluous. Thus, the number

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0$$

may be replaced by the simpler symbol

$$N = (a_m a_{m-1} \cdots a_2 a_1 a_0)_b$$

(the right-hand side is not to be interpreted as a product, but only as an abbreviation for N). We call this the *base b place value notation for N*.

Small values of b give rise to lengthy representation of numbers, but have the advantage of requiring fewer choices for coefficients. The simplest case occurs when the base $b = 2$, and the resulting system of enumeration is called the *binary number system* (from the Latin *binarius*, two). The fact that when a number is written in the binary system only the integers 0 and 1 can appear as coefficients means: every positive integer is expressible in exactly one way as a sum of distinct powers of 2. For example, the integer 105 can be written as

$$\begin{aligned} 105 &= 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^4 + 0 \cdot 2 + 1 \\ &= 2^6 + 2^5 + 2^3 + 1 \end{aligned}$$

or, in abbreviated form,

$$105 = (1101001)_2.$$

In the other direction, $(1001111)_2$ translates into

$$1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 1 = 79.$$

The binary system is most convenient for use in modern electronic computing machines, since binary numbers are represented by strings of zeros and ones; 0 and 1 can be expressed in the machine by a switch (or a similar electronic device) being either on or off.

We ordinarily record numbers in the *decimal system* of notation, where $b = 10$, omitting the 10-subscript which specifies the base. For instance, the symbol 1492 stands for the more awkward expression

$$1 \cdot 10^3 + 4 \cdot 10^2 + 9 \cdot 10 + 2.$$

The integers 1, 4, 9, and 2 are called the *digits* of the given number, 1 being the thousands digit, 4 the hundreds digit, 9 the tens digit, and 2 the units digit. In technical language we refer to the representation of the positive integers as sums of powers of 10, with coefficients at most 9, as their *decimal representation* (from the Latin *decem*, ten).

We are about ready to derive criteria for determining whether an integer is divisible by 9 or 11, without performing the actual division. For this, we need a result having to do with congruences involving polynomials with integral coefficients.

THEOREM 4-4. *Let* $P(x) = \sum_{k=0}^{m} c_k x^k$ *be a polynomial function of* x *with integral coefficients* c_k. *If* $a \equiv b \pmod{n}$, *then* $P(a) \equiv P(b) \pmod{n}$.

Proof: Since $a \equiv b \pmod{n}$, part (6) of Theorem 4-2 can be applied to give $a^k \equiv b^k \pmod{n}$ for $k = 0, 1, \ldots, m$. Therefore

$$c_k a^k \equiv c_k b^k \pmod{n}$$

for all such k. Adding these $m + 1$ congruences, we conclude that

$$\sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k \pmod{n}$$

or, in different notation, $P(a) \equiv P(b) \pmod{n}$.

If $P(x)$ is a polynomial with integral coefficients, one says that a is a solution of the congruence $P(x) \equiv 0 \pmod{n}$ if $P(a) \equiv 0 \pmod{n}$.

COROLLARY. *If* a *is a solution of* $P(x) \equiv 0 \pmod{n}$ *and* $a \equiv b \pmod{n}$, *then* b *is also a solution.*

Proof: From the last theorem, it is known that $P(a) \equiv P(b) \pmod{n}$. Hence, if a is a solution of $P(x) \equiv 0 \pmod{n}$, then $P(b) \equiv P(a) \equiv 0 \pmod{n}$, making b a solution.

One divisibility test that we have in mind is this: A positive integer is divisible by 9 if and only if the sum of the digits in its decimal representation is divisible by 9.

THEOREM 4-5. *Let* $N = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$ *be the decimal expansion of the positive integer* N, $0 \leq a_k < 10$, *and let* $S = a_0 + a_1 + \cdots + a_m$. *Then* $9 \mid N$ *if and only if* $9 \mid S$.

Proof: Consider $P(x) = \sum_{k=0}^{m} a_k x^k$, a polynomial with integral coefficients. The key observation is that $10 \equiv 1 \pmod 9$, whence by Theorem 4-4, $P(10) \equiv P(1) \pmod 9$. But $P(10) = N$ and $P(1) = a_0 + a_1 + \cdots + a_m = S$, so that $N \equiv S \pmod 9$. It follows that $N \equiv 0 \pmod 9$ if and only if $S \equiv 0 \pmod 9$, which is what we wanted to prove.

Theorem 4-4 also serves as the basis for a well-known test for divisibility by 11; to wit, an integer is divisible by 11 if and only if the alternating sum of its digits is divisible by 11. Stated more precisely:

THEOREM 4-6. *Let* $N = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$ *be the decimal representation of the positive integer* N, $0 \leq a_k < 10$, *and let* $T = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m$. *Then* $11 \mid N$ *if and only if* $11 \mid T$.

Proof: As in the proof of Theorem 4-5, put $P(x) = \sum_{k=0}^{m} a_k x^k$. Since $10 \equiv -1 \pmod{11}$, we get $P(10) \equiv P(-1) \pmod{11}$. But $P(10) = N$, whereas $P(-1) = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m = T$, so that $N \equiv T \pmod{11}$. The implication is that both N and T are divisible by 11 or neither is divisible by 11.

Example 4-5

To see an illustration of the last two results, take the integer $N = 1{,}571{,}724$. Since the sum $1 + 5 + 7 + 1 + 7 + 2 + 4 = 27$ is divisible by 9, Theorem 4-5 guarantees that 9 divides N. It can also be divided by 11; for, the alternating sum $4 - 2 + 7 - 1 + 7 - 5 + 1 = 11$ is divisible by 11.

PROBLEMS 4.3

1. Prove the following statements:
   (a) For any integer a, the units digit of a^2 is 0, 1, 4, 5, 6, or 9.
   (b) Any one of the integers 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 can occur as the units digit of a^3.

(c) For any integer a, the units digit of a^4 is 0, 1, 5, or 6.
(d) The units digit of a triangular number is 0, 1, 3, 5, 6, or 8.

2. Find the last two digits of the number 9^{9^9}. [*Hint:* $9^9 \equiv 9 \pmod{10}$, hence $9^{9^9} = 9^{9+10k}$; now use the fact that $9^{10} \equiv 1 \pmod{100}$.]
3. Without performing the divisions, determine whether the integers 176,521,221 and 149,235,678 are divisible by 9 or 11.
4. (a) Obtain the following generalization of Theorem 4-5: If the integer N is represented in the base b by

$$N = a_m b^m + \cdots + a_2 b^2 + a_1 b + a_0, \quad 0 \leq a_k \leq b-1$$

then $b-1 \mid N$ if and only if $b-1 \mid (a_m + \cdots + a_2 + a_1 + a_0)$.
(b) Give criteria for the divisibility of N by 3 and 8 which depend on the digits of N when written in the base 9.
(c) Is the integer $(447836)_9$ divisible by 3 and 8?
5. Using the 9-test or 11-test, find the missing digits in the calculations below:
(a) $52817 \cdot 3212146 = 169655x15282$;
(b) $2x99561 = [3(523 + x)]^2$.
6. Establish the following divisibility criteria:
(a) An integer is divisible by 2 if and only if its units digit is 0, 2, 4, 6, or 8.
(b) An integer is divisible by 3 if and only if the sum of its digits is divisible by 3.
(c) An integer is divisible by 4 if and only if the number formed by its ten and units digits is divisible by 4. [*Hint:* $10^k \equiv 0 \pmod 4$ for $k \geq 2$.]
(d) An integer is divisible by 5 if and only if its units digit is 0 or 5.
7. Show that 2^n divides an integer N if and only if 2^n divides the number made up of the last n digits of N. [*Hint:* $10^k = 2^k 5^k \equiv 0 \pmod{2^n}$ for $k \geq n$.]
8. Let $N = a_m 10^m + \cdots + a_2 10^2 + a_1 10 + a_0$, where $0 \leq a_k \leq 9$, be the decimal expansion of a positive integer N. Prove that 7, 11, and 13 all divide N if and only if 7, 11, and 13 divide the integer

$$M = (100a_2 + 10a_1 + a_0) - (100a_5 + 10a_4 + a_3) + (100a_8 + 10a_7 + a_6) - \cdots.$$

[*Hint:* If n is even, then $10^{3n} \equiv 1$, $10^{3n+1} \equiv 10$, $10^{3n+2} \equiv 100 \pmod{1001}$; if n is odd, then $10^{3n} \equiv -1$, $10^{3n+1} \equiv -10$, $10^{3n+2} \equiv -100 \pmod{1001}$.]
9. Without performing the divisions, determine whether the integer 1,010,908,899 is divisible by 7, 11, and 13.
10. (a) Given an integer N, let M be the integer formed by reversing the order of the digits of N (for example, if $N = 6923$, then $M = 3296$). Verify that $N - M$ is divisible by 9.