Theorem 4.7. If a, b, k, and m are integers such that $k > 0$, $m > 0$, and $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$. .

Proof. Because $a \equiv b \pmod{m}$, we have $m \mid (a - b)$, and because

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}),$$

we see that $(a - b) \mid (a^k - b^k)$. Therefore, by Theorem 1.8 it follows that $m \mid (a^k - b^k)$. Hence, $a^k \equiv b^k \pmod{m}$. ■

Example 4.11. Since $7 \equiv 2 \pmod 5$, Theorem 4.7 tells us that $343 = 7^3 \equiv 2^3 = 8 \pmod 5$. ◄

The following result shows how to combine congruences of two numbers to different moduli.

Theorem 4.8. If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, where $a, b, m_1, m_2, \ldots, m_k$ are integers with $m_1, m_2, \ldots, m_k$ positive, then

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]},$$

where $[m_1, m_2, \ldots, m_k]$ is the least common multiple of $m_1, m_2, \ldots, m_k$.

Proof. Because $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, we know that $m_1 \mid (a - b), m_2 \mid (a - b), \ldots, m_k \mid (a - b)$. By Exercise 39 of Section 3.5 we see that

$$[m_1, m_2, \ldots, m_k] \mid (a - b).$$

Consequently,

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}.$$

■

The following result is an immediate and useful consequence of this theorem.

Corollary 4.8.1. If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, where a and b are integers and $m_1, m_2, \ldots, m_k$ are pairwise relatively prime positive integers, then

$$a \equiv b \pmod{m_1 m_2 \cdots m_k}.$$

Proof. Since $m_1, m_2, \ldots, m_k$ are pairwise relatively prime, Exercise 68 of Section 3.5 tells us that

$$[m_1, m_2, \ldots, m_k] = m_1 m_2 \cdots m_k.$$

Hence, by Theorem 4.8, we know that

$$a \equiv b \pmod{m_1 m_2 \cdots m_k}.$$

■

Modular Exponentiation

In our subsequent studies, we will be working with congruences involving large powers of integers. For example, we will want to find the least positive residue of 2^{644}

modulo 645. If we attempt to find this least positive residue by first computing 2^{644}, we would have an integer with 194 decimal digits, a most undesirable thought. Instead, to find 2^{644} modulo 645 we first express the exponent 644 in binary notation:

$$(644)_{10} = (1010000100)_2.$$

Next, we compute the least positive residues of $2, 2^2, 2^4, 2^8, \ldots, 2^{512}$ by successively squaring and reducing modulo 645. This gives us the congruences

$$\begin{aligned}
2 &\equiv 2 \pmod{645},\\
2^2 &\equiv 4 \pmod{645},\\
2^4 &\equiv 16 \pmod{645},\\
2^8 &\equiv 256 \pmod{645},\\
2^{16} &\equiv 391 \pmod{645},\\
2^{32} &\equiv 16 \pmod{645},\\
2^{64} &\equiv 256 \pmod{645},\\
2^{128} &\equiv 391 \pmod{645},\\
2^{256} &\equiv 16 \pmod{645},\\
2^{512} &\equiv 256 \pmod{645}.
\end{aligned}$$

We can now compute 2^{644} modulo 645 by multiplying the least positive residues of the appropriate powers of 2. This gives

$$2^{644} = 2^{512+128+4} = 2^{512}2^{128}2^4 \equiv 256 \cdot 391 \cdot 16 = 1{,}601{,}536 \equiv 1 \pmod{645}.$$

We have just illustrated a general procedure for *modular exponentiation*, that is, for computing b^N modulo m, where b, m, and N are positive integers. We first express the exponent N in binary notation, as $N = (a_k a_{k-1} \ldots a_1 a_0)_2$. We then find the least positive residues of $b, b^2, b^4, \ldots, b^{2^k}$ modulo m, by successively squaring and reducing modulo m. Finally, we multiply the least positive residues modulo m of b^{2^j} for those j with $a_j = 1$, reducing modulo m after each multiplication.

In our subsequent discussions, we will need an estimate for the number of bit operations needed for modular exponentiation. This is provided by the following proposition.

Theorem 4.9. Let b, m, and N be positive integers such that $b < m$. Then the least positive residue of b^N modulo m can be computed using $O((\log_2 m)^2 \log_2 N)$ bit operations.

Proof. To find the least positive residue of b^N modulo m, we can use the algorithm just described. First, we find the least positive residues of $b, b^2, b^4, \ldots, b^{2^k}$ modulo m, where $2^k \le N < 2^{k+1}$, by successively squaring and reducing modulo m. This requires a total of $O((\log_2 m)^2 \log_2 N)$ bit operations, because we perform $[\log_2 N]$ squarings modulo m, each requiring $O((\log_2 m)^2)$ bit operations. Next, we multiply together the least positive residues of the integers b^{2^j} corresponding to the binary digits of N that are equal to one, and we reduce modulo m after each multiplication. This also requires $O((\log_2 m)^2 \log_2 N)$ bit operations, because there are at most $\log_2 N$ multiplications, each requiring $O((\log_2 m)^2)$ bit operations. Therefore, a total of $O((\log_2 m)^2 \log_2 N)$ bit operations is needed. ■

4.1 Exercises

1. Show that each of the following congruences holds.

a) $13 \equiv 1 \pmod 2$	e) $-2 \equiv 1 \pmod 3$
b) $22 \equiv 7 \pmod 5$	f) $-3 \equiv 30 \pmod{11}$
c) $91 \equiv 0 \pmod{13}$	g) $111 \equiv -9 \pmod{40}$
d) $69 \equiv 62 \pmod 7$	h) $666 \equiv 0 \pmod{37}$

2. Determine whether each of the following pairs of integers is congruent modulo 7.

a) 1,15	d) −1,8
b) 0,42	e) −9,5
c) 2,99	f) −1,699

3. For which positive integers m is each of the following statements true?

a) $27 \equiv 5 \pmod m$
b) $1000 \equiv 1 \pmod m$
c) $1331 \equiv 0 \pmod m$

4. Show that if a is an even integer, then $a^2 \equiv 0 \pmod 4$, and if a is an odd integer, then $a^2 \equiv 1 \pmod 4$.

☞ 5. Show that if a is an odd integer, then $a^2 \equiv 1 \pmod 8$.

6. Find the least nonnegative residue modulo 13 of each of the following integers.

a) 22	d) −1
b) 100	e) −100
c) 1001	f) −1000

7. Find the least positive residue of $1! + 2! + 3! + \cdots + 100!$ modulo each of the following integers.

a) 2	c) 12
b) 7	d) 25

8. Show that if a, b, m, and n are integers such that $m > 0, n > 0, n \mid m$, and $a \equiv b \pmod m$, then $a \equiv b \pmod n$.

9. Show that if a, b, c, and m are integers such that $c > 0$, $m > 0$, and $a \equiv b \pmod m$, then $ac \equiv bc \pmod{mc}$.

10. Show that if a, b, and c are integers with $c > 0$ such that $a \equiv b \pmod c$, then $(a, c) = (b, c)$.

11. Show that if $a_j \equiv b_j \pmod m$ for $j = 1, 2, \ldots, n$, where m is a positive integer and a_j, b_j, $j = 1, 2, \ldots, n$, are integers, then