Example 6.20. We know that $2^{\phi(9)-1} = 2^{6-1} = 2^5 = 32 \equiv 5 \pmod 9$ is an inverse of 2 modulo 9. ◀

We can solve linear congruences using this observation. To solve $ax \equiv b \pmod m$, where $(a, m) = 1$, we multiply both sides of this congruence by $a^{\phi(m)-1}$ to obtain

$$a^{\phi(m)-1}ax \equiv a^{\phi(m)-1}b \pmod m.$$

Therefore, the solutions are those integers x such that $x \equiv a^{\phi(m)-1}b \pmod m$.

Example 6.21. The solutions of $3x \equiv 7 \pmod{10}$ are given by $x \equiv 3^{\phi(10)-1} \cdot 7 \equiv 3^3 \cdot 7 \equiv 9 \pmod{10}$, because $\phi(10) = 4$. ◀

6.3 Exercises

1. Find a reduced residue system modulo each of the following integers.

   a) 6 b) 9 c) 10 d) 14 e) 16 f) 17

2. Find a reduced residue system modulo 2^m, where m is a positive integer.
3. Show that if $c_1, c_2, \ldots, c_{\phi(m)}$ is a reduced residue system modulo m, where m is a positive integer with $m \neq 2$, then $c_1 + c_2 + \cdots + c_{\phi(m)} \equiv 0 \pmod m$.
4. Show that if a and m are positive integers with $(a, m) = (a - 1, m) = 1$, then $1 + a + a^2 + \ldots + a^{\phi(m)-1} \equiv 0 \pmod m$.
5. Find the last digit of the decimal expansion of 3^{1000}.
6. Find the last digit of the decimal expansion of $7^{999,999}$.
7. Use Euler's theorem to find the least positive residue of $3^{100,000}$ modulo 35.
8. Show that if a is an integer such that a is not divisible by 3 or such that a is divisible by 9, then $a^7 \equiv a \pmod{63}$.
9. Show that if a is an integer relatively prime to 32,760, then $a^{12} \equiv 1 \pmod{32,760}$.
10. Show that $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$, if a and b are relatively prime positive integers.
11. Solve each of the following linear congruences using Euler's theorem.

    a) $5x \equiv 3 \pmod{14}$ b) $4x \equiv 7 \pmod{15}$ c) $3x \equiv 5 \pmod{16}$

12. Show that the solutions to the simultaneous system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r}, \end{aligned}$$

where the m_j are pairwise relatively prime, are given by

$$x \equiv a_1 M_1^{\phi(m_1)} + a_2 M_2^{\phi(m_2)} + \cdots + a_r M_r^{\phi(m_r)} \pmod M,$$

where $M = m_1 m_2 \cdots m_r$ and $M_j = M/m_j$ for $j = 1, 2, \ldots, r$.

13. Use Exercise 12 to solve each of the systems of congruences in Exercise 4 of Section 4.3.

14. Use Exercise 12 to solve the system of congruences in Exercise 5 of Section 4.3.

15. Use Euler's theorem to find the last digit in the decimal expansion of 7^{1000}.

16. Use Euler's theorem to find the last digit in the hexadecimal expansion of $5^{1,000,000}$.

17. Find $\phi(n)$ for the integers n with $13 \le n \le 20$.

18. Show that every positive integer relatively prime to 10 divides infinitely many repunits (see the preamble to Exercise 11 of Section 5.1). (*Hint:* Note that the n-digit repunit $111\ldots11 = (10^n - 1)/9$.)

19. Show that every positive integer relatively prime to b divides infinitely many base b repunits (see the preamble to Exercise 15 of Section 5.1).

* 20. Show that if m is a positive integer, $m > 1$, then $a^m \equiv a^{m-\phi(m)} \pmod{m}$ for all positive integers a.

6.3 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica*, or programs you have written, carry out the following computations and explorations.

1. Find $\phi(n)$ for all integers n less than 1000. What conjectures can you make about the values of $\phi(n)$?

2. Let $\Phi(n) = \sum_{i=1}^{n} \phi(n)$. Investigate the value of $\Phi(n)/n^2$ for increasingly large values of n, such as $n = 100$, $n = 1000$, and $n = 10{,}000$. Can you make a conjecture about the limit of this ratio as n grows large without bound?

Programming Projects

Write programs using Maple, *Mathematica*, or a language of your choice to do the following.

1. Construct a reduced residue system modulo n for a given positive integer n.

2. Solve linear congruences using Euler's theorem.

3. Find the solutions of a simultaneous system of linear congruences using Euler's theorem and the Chinese remainder theorem (see Exercise 12).