Linear Congruences: Exercises

1. Find all solutions to the following linear congruences.
   (a) \( 2x \equiv 5 \pmod{7} \).
   (b) \( 6x \equiv 5 \pmod{8} \).
   (c) \( 19x \equiv 30 \pmod{40} \).
   (d) \( 234x \equiv 60 \pmod{762} \).
   (e) \( 128x \equiv 833 \pmod{1001} \).

2. Solve the congruence \( 6789783x \equiv 2474010 \pmod{28927591} \) by any technique of your choosing.

3. Describe the set of all integers \( b \) for which \( 34x \equiv b \pmod{51} \) has solutions.

4. Suppose that it is known that the diophantine equation \( 40x - 622y = 34 \) has complete solution \( x = 2380 + 311t, y = 153 + 20t \). What is the complete solution to the congruence \( 40x \equiv 34 \pmod{622} \)?

5. Given a congruence \( ax \equiv b \pmod{m} \) the properties of congruences guarantee that we can always replace it by an equivalent congruence of the form \( a'x \equiv b' \pmod{m} \) for any \( a' \equiv a \pmod{m} \), \( b' \equiv b \pmod{m} \). How does this observation solve the congruence \( (m - 1)x \equiv b \pmod{m} \) with no work, for any \( m, b \)?

6. (a) Which congruence classes are invertible when \( m = 12 \)?
   (b) Find the inverse of each congruence class in part (a).

7. Find inverses for each invertible congruence class modulo 19.

8. Is it possible for an integer to be equal to its own inverse modulo \( m \)? Illustrate by examples. [Hint: Review the lecture notes!] Can you find an infinite number of examples?

9. Suppose that \( m > 2 \) is an integer. Show that there are always at least two values of \( a \) such that \( a \) is equal to its own inverse modulo \( m \). [Hint: How many solutions does the equation \( x^2 = 1 \) have in the real number system? Which of those solutions carry over in modular arithmetic?]

10. Prove that if \( p \) is prime then any integer \( a \) which is not divisible by \( p \) is invertible mod \( p \).

11. Prove that for a positive integer \( m \), an integer \( a \) is invertible mod \( m \) iff \( \gcd(a, m) = 1 \).
12. Explain how to use the Euclidean algorithm to find an inverse of any invertible congruence class mod \( m \).

13. Compute the following modular inverses, if possible.
   
   (a) \( 80^{-1} \text{ mod } 171 \).
   (b) \( 200^{-1} \text{ mod } 171 \).
   (c) \( 87^{-1} \text{ mod } 171 \).
   (d) \( 171^{-1} \text{ mod } 200 \).
   (e) \( 97^{-1} \text{ mod } 200 \).

14. Use the modular inverses found in the preceding problem to solve the following congruences, if possible, by multiplying by the inverse.
   
   (a) \( 80x \equiv 51 \text{ (mod } 171 \).)
   (b) \( 200x \equiv 73 \text{ (mod } 171 \).)
   (c) \( 87x \equiv 73 \text{ (mod } 171 \).)
   (d) \( 171x \equiv 79 \text{ (mod } 200 \).)
   (e) \( 97x \equiv 173 \text{ (mod } 200 \).)

15. Solve the congruence \( 513x \equiv 237 \text{ (mod } 600 \), if possible, by first reducing it to an equivalent congruence that can then be solved by multiplication by a modular inverse.

16. Discuss the sense in which a modular inverse is unique, or explain why this makes no sense.

17. Use the method of modular inverses to solve the following linear congruences, if possible.
   
   (a) \( 501x \equiv 1218 \text{ (mod } 1689 \).)
   (b) \( 123456789x \equiv 90909090 \text{ (mod } 987654321 \).)

   In what sense is (b) actually easier than (a), despite appearances?