Homework 2 for Modular Arithmetic

Math-270: Discrete Mathematics

January 10, 2018

Questions

1. Using the Cayley Tables, how many solutions are there to $10x = 15 \bmod 25$?
2. Using the Cayley Tables, how many solutions are there to $10x = 11 \bmod 25$?
3. Based on the previous two questions, do you think 10 is invertible mod 25?
4. Using the Cayley Tables, how many solutions are there to $11x = 15 \bmod 25$?
5. Using the Cayley Tables, how many solutions are there to $11x = 14 \bmod 25$?
6. Based on the previous two questions, do you think 11 is invertible mod 25?
7. Using the Cayley Tables, what is the inverse of 4 mod 11?
8. Using the Cayley Tables, what is the inverse of 5 mod 11?
9. Using the Cayley Tables, what is the inverse of 6 mod 11?
10. Using the Cayley Tables, what is the inverse of 7 mod 11?
11. Let $f(x) \equiv 2x + 5 \bmod 11$. Solve $f(x) \equiv 1$ for x, working mod 11.
12. Let $g(x) \equiv 17x + 19 \bmod 25$. Solve $g(x) \equiv 15$ for x, working mod 25.
13. Let $h(x) \equiv 13x + 11 \bmod 17$. Solve $h(x) \equiv 8$ for x, working mod 17.
14. When is an integer k, with $0 < k < N$, invertible modulo N?
15. What is the gcd of 60 and 48?
16. What is the gcd of 32 and 48?
17. What is the gcd of 49 and 48?
18. What is the gcd of 60 and 50?
19. What is the gcd of 60 and 63?
20. What is the gcd of 60 and 61?
21. Which of the above pairs of numbers (in Problems 15–20) qualify as a pair of relatively prime numbers?
22. If I know that $(15)(8) + (-7)(17) = 1$ what does that tell me about the inverse of 8 mod 17?
23. If I know that $(-15)(9) + (8)(17) = 1$ what does that tell me about the inverse of 9 mod 17?
24. If I know that $(-5)(10) + (3)(17) = 1$ what does that tell me about the inverse of 10 mod 17?
25. Provide a Bezout Equation for 4 and 15. Write your answer as an equation $ax + by = g$.
26. Provide a Bezout Equation for 5 and 15. Write your answer as an equation $ax + by = g$.
27. Provide a Bezout Equation for 6 and 15. Write your answer as an equation $ax + by = g$.
28. Provide a Bezout Equation for 7 and 15. Write your answer as an equation $ax + by = g$.
29. Looking at Problem 25, what is the inverse of 4 mod 15?
30. Looking at Problem 28, what is the inverse of 7 mod 15?
31. What is the inverse of 4 mod 19? Hint: use $a(4) + b(19) = 1$ to help you.
32. What is the inverse of 5 mod 19? Hint: think about your answer to the previous problem.
33. What is the inverse of 6 mod 19? Hint: use $a(6) + b(19) = 1$ to help you.

Answers

1. There are five solutions.
2. There are no solutions.
3. Definitely not. One counter-example is enough, but here we have two, which is extra.
4. There is one solution.
5. There is one solution.
6. Yes, it appears to be so, though two examples does not qualify as a proof.
7. The inverse of 4 mod 11 is 3.
8. The inverse of 5 mod 11 is 9.
9. The inverse of 6 mod 11 is 2.
10. The inverse of 7 mod 11 is 8.
11. $f(9) \equiv 1 \bmod 11$.
12. $g(13) \equiv 15 \bmod 25$.
13. $h(5) \equiv 8 \bmod 17$.
14. An integer k with $0 < k < N$ is invertible modulo N if and only if k is coprime to N. (Remember, coprime and relatively prime are synonyms.)
15. 12
16. 16
17. 1
18. 10
19. 3
20. 1
21. 60 is relatively prime to 61; 49 is relatively prime to 48.
22. The inverse of 8 mod 17 is 15.
23. The inverse of 9 mod 17 is 2, because $-15 + 17 = 2$.
24. The inverse of 10 mod 17 is 12, because $-5 + 17 = 12$.
25. One equation is $4(4) + (-1)(15) = 1$. This makes sense because $\gcd(4, 15) = 1$. Other equations include $19(4) + (-5)(15) = 1$ as well as $-11(4) + (3)(15) = 1$. Remember, there is an infinite number of equations that work.
26. One equation is $4(5) + (-1)(15) = 5$. This makes sense because $\gcd(5, 15) = 5$. Other equations include $19(5) + (-6)(15) = 5$ as well as $-11(5) + (4)(15) = 5$. Remember, there is an infinite number of equations that work.
27. One equation is $-2(6) + 1(15) = 3$. This makes sense because $\gcd(6, 15) = 3$. Other equations include $13(6) + (-5)(15) = 3$ as well as $-17(6) + (7)(15) = 3$. Remember, there is an infinite number of equations that work.
28. One equation is $-2(7) + 1(15) = 1$. This makes sense because $\gcd(7, 15) = 1$. Other equations include $13(7) + (-6)(15) = 1$ as well as $-17(7) + (8)(15) = 1$. Remember, there is an infinite number of equations that work.
29. Since $4(4) + (-1)(15) = 1$, we reduce mod 15, and get $(4)(4) + (-1)(0) \equiv 1 \bmod 15$ or $(4)(4) \equiv 1 \bmod 15$, and therefore 4 is the inverse of 4. Check: $4(4) = 16 = 15 + 1 \equiv 1 \bmod 15$.
30. Since $-2(7) + 1(15) = 1$, we reduce mod 15, and get $(13)(7) + 1(0) \equiv 1 \bmod 15$ or $(13)(7) \equiv 1 \bmod 15$, and therefore 13 is the inverse of 7. Check: $13(7) = 91 = 90 + 1 = 6(15) + 1 \equiv 1 \bmod 15$.
31. The inverse of 4 mod 19 is 5.
32. The inverse of 5 mod 19 is 4. Remember, $(4)(5) \equiv 1 \bmod 19$ means that "4 and 5 are inverses" mod 19. The relationship goes both ways.
33. The inverse of 6 mod 19 is 16.