

Homework 1 for Modular Arithmetic

Math-270: Discrete Mathematics

January 10, 2018

Questions

1. What is $(8)(7) \bmod 11$?
2. What is $(9)(11) \bmod 25$?
3. What is $(14)(13) \bmod 17$?
4. What is $7(9) + 3 \bmod 11$?
5. What is $8(17) - 5 \bmod 25$?
6. What is $5(9) - 11 \bmod 17$?
7. Evaluate $h(x) \equiv 9x + 4 \pmod{17}$ at $x = 11$.
8. Evaluate $f(x) \equiv 2x + 5 \pmod{11}$ at $x = 4$.
9. Evaluate $g(x) \equiv 17x + 19 \pmod{25}$ at $x = 5$.
10. Which of these is a valid ISBN code?
 - 0-321-57198-4
 - 0-321-57189-4
 - 0-321-67189-4
11. Look at the Cayley table for mod 26. The multiplication table is given, but the addition table is not. There is also an alphabet there, with twenty-six letters mapped to the integers mod 26. We can define the affine cipher as follows. First, change the letters to numbers. Second, put the number into a function, such as $f(x) = 17x + 19 \pmod{26}$. Third, change the output of that function back into a letter.
 - (a) Using $f(x) = 17x + 19$, encrypt FROG.
 - (b) Using $f(x) = 17x + 19$, encrypt BEER.
 - (c) Using $g(x) = 13x + 3$, encrypt BEER.
 - (d) Using $g(x) = 13x + 3$, encrypt BOAT.
 - (e) Using $h(x) = 23x + 5$, encrypt AWXR.
 - (f) Using $h(x) = 23x + 5$, encrypt KJJW.
 - (g) Based on (c) and (d), do you think $g(x)$ is a good cipher?
 - (h) Based on (c) and (d), do you think $g(x)$ is injective?

Note: The affine cipher is a toy cipher meant to train us in cryptography. It is less secure than the secret-decoder ring in a cracker-jack box. Don't use it in practice.

Answers

1. $(8)(7) \equiv 1 \pmod{11}$.
2. $(9)(11) \equiv 24 \pmod{25}$.
3. $(14)(13) \equiv 12 \pmod{17}$.
4. $7(9) + 3 \equiv 0 \pmod{11}$.
5. $8(17) - 5 \equiv 6 \pmod{25}$.
6. $5(9) - 11 \equiv 0 \pmod{17}$.
7. $h(11) = 9(11) + 4 = 99 + 4 = 103 = 102 + 1 = 6(17) + 1 \equiv 1 \pmod{17}$.
8. $f(4) \equiv 2 \pmod{11}$.
9. $g(5) \equiv 4 \pmod{25}$.
10. The ISBN codes...
 - 0-321-57198-4 is invalid.
 - 0-321-57189-4 is valid.
 - 0-321-67189-4 is invalid.

Note: As you can see, the first ISBN is just the second ISBN with the 8 and 9 swapped. But the ISBN code system detected this.

Note: As you can see, the third ISBN is just the second ISBN with the 5 replaced by a 6. But the ISBN code system detected this.

Note: It really is an error-detecting code!

11. Now, the affine cipher.
 - (a) (F, R, O, G) becomes (5, 17, 14, 6) and $(f(5), f(17), f(14), f(6)) \equiv (0, 22, 23, 17)$, which is (A, W, X, B) or “AWXR.”
 - (b) (B, E, E, R) becomes (1, 4, 4, 17) and $(f(1), f(4), f(4), f(17)) \equiv (10, 9, 9, 22)$, which is (K, J, J, W) or “KJJW.”
 - (c) (B, E, E, R) becomes (1, 4, 4, 17) and $(g(1), g(4), g(4), f(17)) \equiv (16, 3, 3, 16)$, which is (Q, D, D, Q) or “QDDQ.”
 - (d) (B, O, A, T) becomes (1, 14, 0, 19) and $(g(1), g(14), g(0), f(19)) \equiv (16, 3, 3, 16)$, which is (Q, D, D, Q) or “QDDQ.”
 - (e) (A, W, X, R) becomes (0, 22, 23, 17) and $(h(0), h(22), h(23), h(17)) \equiv (5, 17, 14, 6)$, which is (F, R, O, G) or “FROG.”
 - (f) (K, J, J, W) becomes (10, 9, 9, 22) and $(h(10), h(9), h(9), h(22)) \equiv (1, 4, 4, 17)$, which is (B, E, E, R) or “BEER.”

Note: In cryptography we say that if $f(x)$ is our encryption function, then $g(x)$ is our decryption function.

(g) Hell no. If a military unit is in urgent need of a boat, and they get a beer instead, then that’s a major problem.

(h) Clearly not. We had several cases of differing inputs getting the same output.

Note: Amazingly, in any environment with a finite domain and range of equal size, a function is either all three (injective, surjective, and bijective) or none of the three. It is okay if this surprises you, because I didn’t teach that.

Note: Since (c) and (d) show that the cipher is not injective (and therefore not surjective or bijective), then we know that it cannot be inverted. Since it cannot be inverted, then the message cannot be read by the intended recipient. For this reason, we require all encryption functions to be injective, and we call this “unique decodability.”