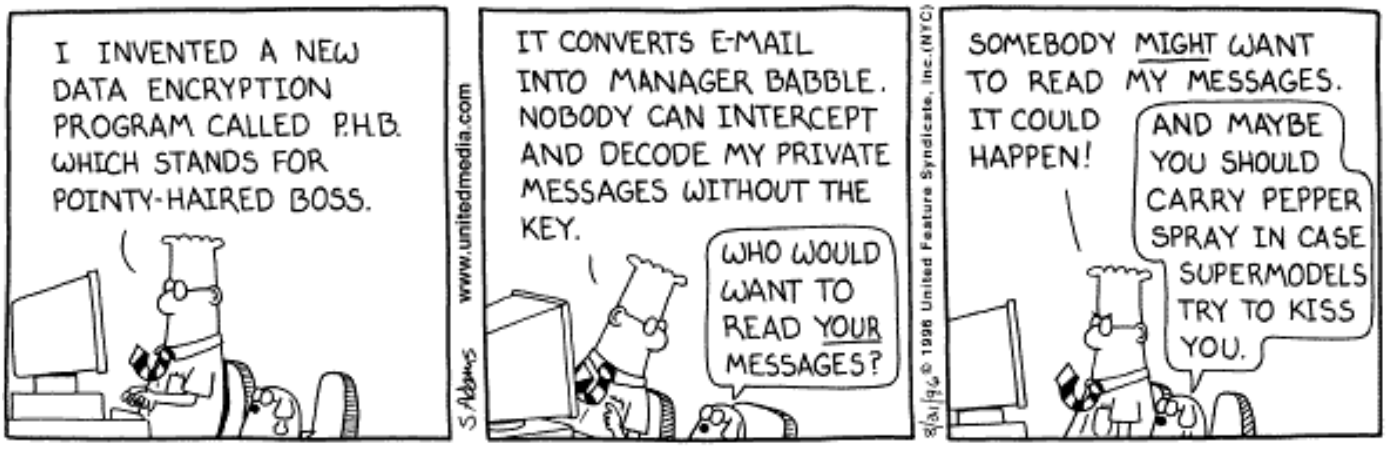
Homework #1

Modular Addition and Functions

Out : September 9, 2:30pm

Due : September 16, 12:30pm

Instructions: Please turn in homework neatly written on separate, lined paper (except for the table from problem 4a), to the CS007 handin bin in CIT room 242.



1. Do each of the following problems with the given modulus and write x in standard form.

   (a) $x \equiv 4 + 3 \pmod 8$

   (b) $x \equiv 7 + 34 \pmod 4$

   (c) $13 + 22 \equiv x \pmod{13}$

   (d) $6 - 7 \equiv x \pmod{88}$

   (e) $x \equiv 9 - 19 \pmod 7$

   (f) $12 + 4 + 7 + 12 + 17 \equiv x \pmod{12}$

   (g) $7 + x \equiv 2 \pmod 3$

2. Explain your answers to the following questions. Today is Wednesday.

   (a) What day will it be in 7 days?

   (b) In 67 days what day will it be?

   (c) If a government proposal were passed to lengthen the weekend by sticking in an extra day after Saturday, what day would it be 67 days from now?

3. Examine the number 4.51283512835128351283.... What is the 295th digit after the decimal point in this number? Explain how you got your answer.

4. We played the game NIM in class. It is the games where you and your opponent have a bunch of pennies spread out in front of you and the two of you take turns taking either 1, 2 or 3 pennies. Your goal is to force your opponent to take the last penny.

   (a) Now consider a modified version of the game: instead of taking 1, 2, or 3 pennies, you can now take either 1, 2, 3, or 4 pennies, but you still want your opponent to take the last penny. Fill in the rest of the table on the following page and *turn this page in* with the rest of your answers.

   (b) Explain using the concept of a modulus what number of pennies you want to leave for your opponent after you take your turns.

5. Remember that the encryption function for the Caesar cypher looks like this: $f(plain, key) = (plain + key)$ rem 26. Let $g(cyph, key)$ be the decryption function. That is, for a cyphertext $cyph$, $g(cyph, key)$ is the corresponding cleartext symbol.

   (a) Give the rule for g. ($g(cyph, key) = ...?$)

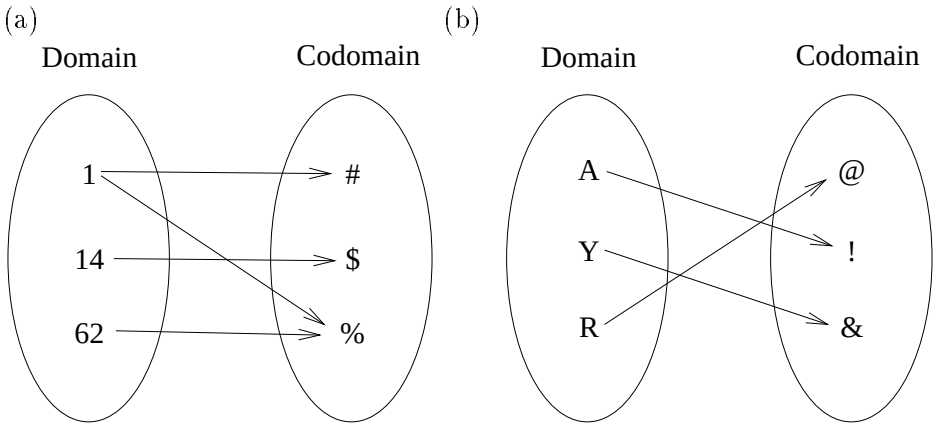
   (b) Suppose you are Eve, the eavesdropper. You intercept the following symbol of cyphertext: "L". You know that it was encrypted using the Caesar cypher, but you don't know the key. Enumerating all the keys, determine all the possible decryptions.

   (c) Now consider the use of the encryption function as the basis for a block cypher. That is, encrypt (or decrypt) each symbol of the cleartext seperately. Suppose you, again Eve, intercept the following cyphertext which you know has been encrypted with a block cypher based on the Caesar cypher. Given that the cleartext is English text, how might you go about decrypting this message?

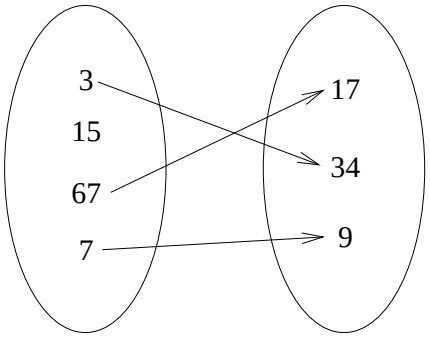
      KYVVCVGYREKZJREXIP.

   (d) Suppose now that you have learned that the key is 17. What is the cleartext?

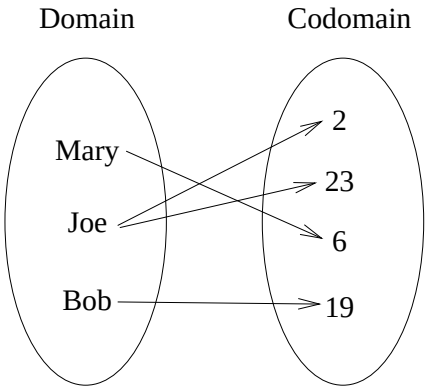
6. For each of the following diagrams, state whether it is or is not a function.



(c)

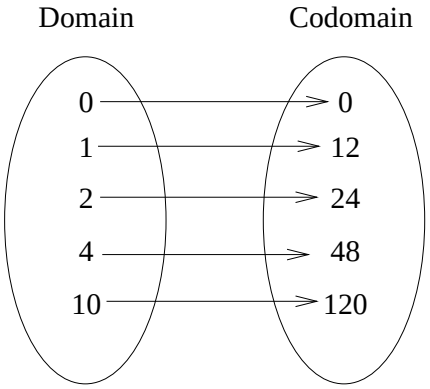


(d)

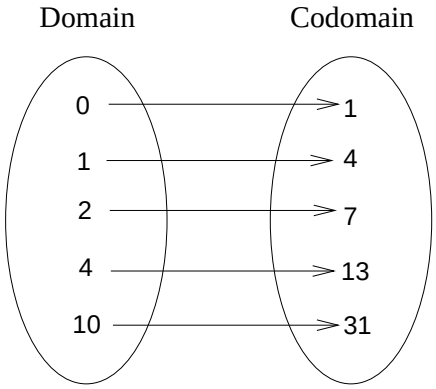


7. For each of the following diagrams, give the rule to which it corresponds.

(a)



(b)

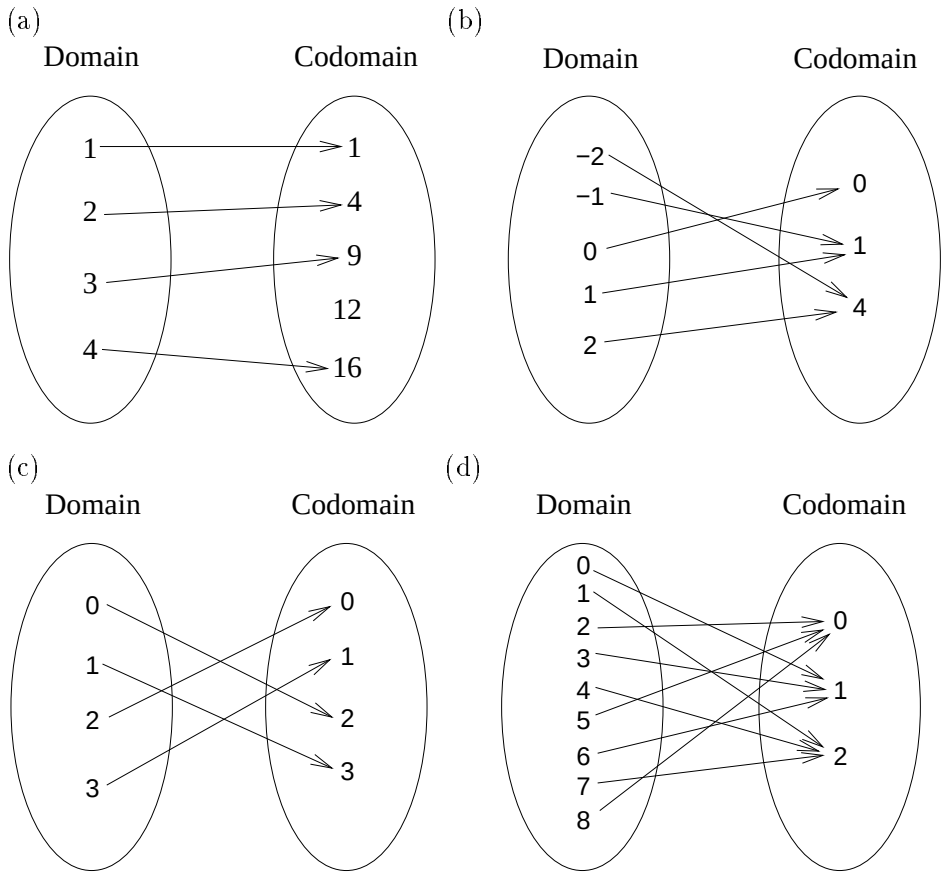


8. Consider the functions depicted in problem 7.

   (a) Give the rule for the inverse of the function in 7(a).

   (b) Do the same for 7(b).

9. Give the rule for the following diagrams:



10. Consider the diagrams in problem 9. For each, give the rule for the inverse or, if the diagram has no inverse, explain why this is the case. (The concepts of one-to-one and onto might be useful here.)

11. Assume you are using an alphabet that contains only four characters/symbols (Say, "A", "B", "C", and "D").

    (a) How many different Caesar cyphers can be used with this alphabet? (ie, how large is the keyspace?)

    (b) How many different possible substitution keys exist for this alphabet?

12. For each of the following communication scenarios, give a brief argument for or against the security of that channel. Note: this does not need to be technical. We don't have specific answers in mind for this question.

    (a) Placing a credit-card order over the telephone.

    (b) Withdrawing cash from an ATM.

    (c) Paying a utility bill by mail.

    (d) Sending email to your professor.

13. Your eternal archnemesis, Eve, has joined the cs007 TA staff. Given this fact, explain, in your own words, what kinds of risks you are taking by running the MarkCalc. Again, your answer need not be technical.

Table for problem 4a:

# of Pennies Left	You Win/Lose	Strategy
1	Lose	None
2	Win	Take one penny.
3	Win	Take two pennies.
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		