CS 4920/5920 Spring 2022
HW 2

HW 2 is due on 2/23. Explain how you reached your answers. Answers without explanations will receive no to little credit.

If you use programming to compute the values for the Euclidean Algorithm and Extended Euclidean Algorithm problems, submit a zip file including your answer sheet/doc/pdf and your code and files.

Problem 1. Dice

In each *event*, you throw a dice and observe the number.

a. You are using a typical dice. What is the information entropy value for one event? What is the entropy value for four events?
b. Now suppose you modify the dice so that the sides that originally showed number six and four become five's (the numbers 1, 2, 3 occupy one side each, and 5 occupies three sides). What is the information entropy for one event? What is the entropy for five events?
c. You can further modify the dice by changing the numbers it shows on the sides. How would you maximize the entropy?
d. You can further modify the dice by changing the numbers it shows on the sides. How would you minimize the entropy?
e. You use two typical dice (each showing 1, 2, 3, 4, 5, 6 in the sides). You throw the two dice and observe the sum. What is the information entropy of this event?

Problem 2. Balls in a Bin

Suppose there are three red balls, two yellow balls, and four green balls in a bin. In each *event*, you pick one ball from the bin and observe the color of the ball (the balls are only distinguishable by their colors). After observation, you put the ball back into the bin.

a. What is the information entropy value for an event?
b. What is the information entropy for n events where n is a positive integer?
c. Now you add one red ball and one yellow ball in the bin and conduct the events. What is the value of the entropy for an event?
d. Suppose there are only three colors: red, yellow, and green. From Part c. (with a total of eleven balls in the bin), you can either add one ball of any color to the bin or subtract one ball of any color from the bin. What would your action be (add or subtract and which color) to *maximize* the entropy of the events?
e. Suppose there are only three colors: red, yellow, and green. From Part c. (with a total of eleven balls in the bin), you can either add one ball of any color to the bin or subtract one ball of any color from the bin. What would your action be (add or subtract and which color) to *minimize* the entropy of the events?
f. Suppose now you can choose any color beyond red, yellow, and green. From Part c. (with a total of eleven balls in the bin), you can either add one ball of any color to the bin or subtract one ball of any color from the bin. What would your action be (add or subtract and which color) to *maximize* the entropy of the events?

Problem 3.

Prove the followings:

a. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$

b. [(a mod n) - (b mod n)] mod n = (a - b) mod n
c. For two consecutive integers n and n+1, GCD(n,n+1)=1

Problem 4.
This problem is about the Euclidean Algorithm.

a. State and prove the Euclidean Algorithm.

Then, use Euclidean Algorithm to solve the following. Provide a table similar to Table 2.1 in the textbook. Alternatively, you can write a computer program to generate the table; if you do so, describe your program and include your code (and the compiler output if applicable) in zip for your homework submission.

b. GCD(1105,425)
c. GCD(2078,9602)
d. GCD(22142,16762)

Problem 5.
This problem is about the Extended Euclidean Algorithm.

a. State and prove the Extended Euclidean Algorithm.

Then, using the extended Euclidean algorithm, find the multiplicative inverse of the following. Provide a table similar to Table 2.4 in the textbook. Alternatively, you can write a computer program to generate the table values; if you do so, describe your program and include your code (and the compiler output if applicable) in zip for your homework submission.

a. 650 mod 1769
b. 950 mod 1767
c. 10012 mod 234378

Problem 6.

a. For a block of n bits, the number of different reversible mappings for the ideal block cipher is $2^n!$. Justify and explain.
b. For the ideal block cipher, allowing all possible reversible mappings, the size/length of the key is $n \times 2^n$ bits. However, if there are $2^n!$ possible mappings, it should take $\log_2(2^n!)$ bits to discriminate among the different mappings, and so the key length should be $\log_2(2^n!)$ bits. However, $\log_2(2^n!) < n \times 2^n$. Explain the discrepancy.