# CSCI 1311: Problem Set 5

Due: Apr. 3, 2020

---

**Instructions**:

> Your submission must be **typed** and submitted to gradescope as a single pdf. You **may not** submit handwritten pictures via gradescope.

- You must include a cover page, that contains your name, the assignment information, the date, and your GW email address. No answers to questions should appear on the cover page.
- Try and organize your submission such that answers to questions (or parts of questions) do not span multiple pages. This will make it much easier to grade. **Ideally, each page will start with a new question (or part of question). See the sample for PS0 for a nice easy formatting.**
- On gradescope, be sure to mark which page your answer to each question (or sub question) is located. Doing so inaccurately could lead to issues with grading.

---

**Question Weighting**

| Question: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Total |
|---|---|---|---|---|---|---|---|---|---|
| Points: | 10 | 6 | 19 | 20 | 20 | 25 | 10 | 0 | 110 |

This problem set is graded out of 100 points, scores above 100 points are allowed and considered bonus.

---

1. **[10 points]** Prove that for all integers $n \geq 1$, $R$ is an equivalence relation:

$$a\,R\,b \iff a \equiv b \pmod{n}$$

2. Find the multiplicative inverse of each of the following modulo 7:
   (a) **[2 points]** 5
   (b) **[2 points]** 6
   (c) **[2 points]** 493

3. Consider the following RSA keys, $pq = 55$, $e = 3$ and $d = 27$, and an alphabetic encoding where each letter of the alphabet is mapped to its number, where $1$ is $A$, and $2$ is $B$ and so on.
   (a) **[4 points]** Encrypt the message "STAY" using the RSA keys.
   (b) **[15 points]** Decrypt the cyphertext $\{15, 25, 52, 10\}$
   (***Note: that if you write a program to do*** $x^{27}$ ***it may overflow the integer leading to the wrong answer, so you need to compute smaller results taking advantage of the modular arithmetic. Show your work.***)

4. For this question, consider 6 digit PINs that contain the numbers 0-9 for each digit.
(***Writing a number is not sufficient, show your work and the formula you used to reach that conclusion!***)
   (a) **[1 point]** How many 6-digit PINs with repetitions are there?
   (b) **[2 points]** How many 6-digit PINs are there where numbers cannot repeat?
   (c) **[3 points]** How many 6-digit PINs without repetitions are there where the first digit must be a 5 and the last must be a 7 ?
   (d) **[4 points]** How many 6-digit PINs with repetitions are there that have at least one digit is a 7?
   (e) **[10 points]** How many 6-digit PINs with repetition are there that have at least one digit that is a 7 **or** at least one digit that is a 5.

5. **[20 points]** ***Choose one of the following two problems to complete, or do both for a 5 point bonus if you are correct on both of them.*** You must clearly indicate which you want graded first, and only if the first one is correct will the second one be considered.

   Again, consider 6 digit PINs that can contain numbers 0-9 for each digit.
(***Writing a number is not sufficient, show your work and the formula you used to reach that conclusion!***)
   (a) How many 6-digit PINs with repetition of digits are there where at least *two* digits are a 7?
   (b) How many 6-digit PINs with repetition of digits are there that have at least one 7 **and** at least one 5?

6. Consider a urn of balls: 4 balls are blue, 6 balls are red, and 10 balls are yellow. (***Writing a number is not sufficient, show your work and the formula you used to reach that conclusion!***)
   (a) **[5 points]** You draw five balls from the urn, what is the probability of drawing all red balls *or* all yellow balls?
   (b) **[5 points]** If you draw two balls from the urn, what is the probability that you draw at least one yellow ball?
   (c) **[15 points]** Assume you draw three balls, if at least one of the balls were red, what is the probability that the other two balls you've drawn are also red?

7. **[10 points]** You're playing "Let's make a deal, 2.0" and on this version of the game show, there is a game with **4 doors!** Behind two of the doors is a goat, behind one door is a car, and behind a third door is a *sweet* road bike. You're goal is to win a car or the *sweet* road bike.

   Like in the game before, you get to make an initial selection of one of the doors, and for example, let's assume that it is door #1. The game show host than reveals to you the location whats behind one of the doors, always revealing a goat. Let's say that the door revealed is door #2.

   Now, the host asks you a question: Would you like to swap to one of the other remaining unrevealed doors? That is door #3 and door #4. Should you swap or stay?

   Provide an argument, for why you should either swap or stay. Your answer should include concrete probabilities for either swapping to another door or staying with your initial door with respect to winning the car or the *sweet* road bike.

8. **[10 bonus points]** Find the answer to the difficult question at the end of Lecture 15.