EE 418 - Assignment 1

Total Points: 100
Autumn Quarter, 2021
Prof. Radha Poovendran
Department of Electrical and Computer Engineering
University of Washington, Seattle, WA 98195

Due: 11:59 pm (PST) on Oct 21 (Thur), 2021 via Canvas

Note:

- This homework contains both computation questions (marked as **[Com]**) which are required to do by hand calculations and programming questions (marked as **[Pro]**) which are required to write Python /MATLAB codes. Zero points will be awarded if **[Com]** questions are solved via Python/MATLAB scripts and if **[Pro]** questions are solved by hand calculations.
- Show the computation steps and/or justify your answers in all the **[Com]** questions. Failure to show any intermediate computation steps in **[Com]** questions will result zero points.
- You can use and modify the Python functions provided in the file section of the EE 418 canvas page when answering the **[Pro]** questions.
- For problem 3, you are encouraged to collaborate with one classmate and work together and provide the answers. In your submission, please write the first and the last name of the classmate you worked with. For all other problems, you can discuss with others but you need to write your own computation steps, justifications and/or Python/MATLAB codes.
- **Your answers to this homework must be submitted through canvas as a single zip file containing the following:** *i*) **hand written and scanned or word or pdf answers to all the computational and discussion questions as single pdf file.** *ii*) **Python/MATLB codes for programming questions as in filename.py or filename.m respectively.**
- **Name of your submission zip file should follow the following format. "*#_$_EE418_HW1.zip*", where "#" and "$" should be replaced with your first name and last name, respectively.**

1. **[Com]** (Modulo Addition, 2 pts x 6 = 12 pts) Please find *i*) $(a + b) \pmod m$ and *ii*) $a \pmod m$, $b \pmod m$ and $(a \pmod m) + b \pmod m)) \pmod m$ for each values of a, b and m given below. You are allowed to use calculators or Python codes provided in the class. However, your answers must include the computaion steps as shown below.

   e.g., $a = 15$, $b = 28$, and $m = 10$
   Ans: (i) $(15 + 28) \pmod{10} = 43 \pmod{10} = 3 \pmod{10}$
   (ii) $15 \pmod{10} + 28 \pmod{10} = 5 \pmod{10} + 8 \pmod{10} = 13 \pmod{10} = 3 \pmod{10}$

   (a) $a = 35$, $b = 256$ and $m = 10$
   (b) $a = -300$, $b = -93$ and $m = 26$
   (c) $a = 10496$, $b = -5899$ and $m = 256$
   (d) $a = 771$, $b = 400375$ and $m = 1024$
   (e) $a = -37388$, $b = 509$ and $m = 4096$
   (f) $a = -25678$, $b = -895632$ and $m = 33558$

2. **[Com]** (Modulo Multiplication, 2 pts x 6 = 12 pts) Please find *i*) $(a \cdot b) \pmod m$ and *ii*) $a \pmod m$, $b \pmod m$ and $(a \pmod m) \cdot b \pmod m)) \pmod m$ for each values of a, b and m given below. You are allowed to use calculators or Python codes provided in the class. However, your answers must include the computaion steps as shown below.

   e.g., $a = 15$, $b = 28$, and $m = 10$
   Ans: (i) $(15 \cdot 28) \pmod{10} = 420 \pmod{10} = 0 \pmod{10}$
   (ii) $15 \pmod{10} \cdot 28 \pmod{10} = 5 \pmod{10} \cdot 8 \pmod{10} = 40 \pmod{10} = 0 \pmod{10}$

   (a) $a = 432$, $b = 163$ and $m = 12$
   (b) $a = -531$, $b = -435$ and $m = 26$
   (c) $a = -2465$, $b = 8526$ and $m = 512$
   (d) $a = 1024$, $b = 400375$ and $m = 2048$
   (e) $a = -45599$, $b = 7999$ and $m = 8192$
   (f) $a = -4536783$, $b = -39632$ and $m = 47384$

3. (GCD and Modulo Inverse) Please answer the following questions.

   (a) **[Pro]** (5 pts) Please write a Python/MATLAB function to calculate gcd of three integers a, b, and c.

   (b) **[Pro]** (1 pts x 3 = 3 pts) Use the function you developed in part (a) to find the gcd of the following integer values a, b, and c.
   - $a = -144$, $b = 2058$, $c = 302526$
   - $a = 3674160$, $b = -243$, $c = 51030$
   - $a = -733$, $b = -21379$, $c = 46782$

(c) **[Com]** (2 pts x 5 = 10 pts) Please find *i*) $(a^{-1}) \pmod m$ and *ii*) $a \pmod m$ and $(a \pmod m)^{-1} \pmod m$ for each values of a and m given below. You are allowed to use calculators or Python codes provided in the class. However, your answers must include the computaion steps as shown below.

> e.g., $a = 33$ and $m = 10$
> Ans: $\gcd(33, 10) = 1$. Therefore, $33^{-1} \pmod{10}$ exists.
> (i) $33^{-1} \pmod{10} = 7 \pmod{10}$
> (ii) $(33 \pmod{10})^{-1} \pmod{10} = 3^{-1} \pmod{10} = 7 \pmod{10}$

- $a = 777$, and $m = 26$
- $a = -37$, and $m = 512$
- $a = 24865$, and $m = 4096$
- $a = -256789$, and $m = 56789$
- $a = -1900757$, and $m = 770077$

(d) **[Pro]** (5 pts) Find out how much time is taken to calculate inverses in each of the cases in part *c*). For example if you are using "modulo_inverse_naive" python function provided in the "Mapping English Alphabet to Integers And Modulo Arithmetic" notebook, you may use the following code to calculate run time.

```
import time
n = -1923
m = 3457684
start_time = time.time()
modulo_inverse_naive(n,m,1)
end_time = time.time()
print("Run time in seconds (s):",(end_time - start_time))
```

```
Inverse of -1923 in mod 3457684 is 1409685
Run time in seconds (s): 2.433605194091797
```

Figure 1: Sample python code for calculating run time associated with "modulo_inverse_naive" python function provided in the "Mapping English Alphabet to Integers And Modulo Arithmetic" notebook.

(e) **[Com]** (5 pts) Do you observe any specific pattern in the run times computed in part *d*)? If so, briefly explain the reason for your observations in part *d*.

4. **[Com]** (Modulo Arithmetic, 3 pts x 6 = 18 pts) Please find the answers for the following questions using the properties of modulo arithmetic. You are allowed to use calculators or Python codes provided in the class. However, your answers must include the computaion steps as shown below.

> e.g., $(33^{-1} \cdot 12 - 14^2) \pmod{10}$
> Ans: $\gcd(33, 10) = 1$. Therefore, $33^{-1} \pmod{10}$ exists.
> $(33 \pmod{10})^{-1} \cdot 12 \pmod{10} - (14 \pmod{10})^2 = (3^{-1} \pmod{10}) \cdot (2 \pmod{10}) - 4^2 \pmod{10}$
> $= (7 \pmod{10}) \cdot (2 \pmod{10}) - 16 \pmod{10} = 14 \pmod{10} - 6 \pmod{10}$
> $= 4 \pmod{10} - 6 \pmod{10} = -2 \pmod{10} = 8 \pmod{10}$.

(a) $(32 \cdot (-71) + 782) \pmod 7$

(b) $(-534 \cdot (90 + 4382)) \pmod{26}$

(c) $((-543 - 4652) \cdot (-75 + 976)) \pmod{256}$

(d) $(3113^2 \cdot (-782)) \pmod{2048}$

(e) $((-5)^4 \cdot 2153^{-3}) \pmod{4096}$

(f) $(((-35 \cdot 3) + 7762)^{-7} \cdot ((-5462)^2 - (2161)^{-1})^5) \pmod{12235}$

5. (Permutation Cipher)

   (a) **[Com]** (5 pts) [(a)] Suppose that π is the following permutation of $\{1, ..., 8\}$:

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	1	6	2	7	3	8	5

   Compute the permutation π^{-1}.

   (b) **[Pro]** (10 pts) [(b)] Write a Python/MATLAB function for permutation cipher decryption with $m = 8$. This function will take the ciphertext (y) and permutation key ($\pi(x)$) as inputs and output plaintext (x).

   (c) **[Pro]** (5 pts) [(c)] Decrypt the following ciphertext, for a *Permutation Cipher* with $m = 8$, which was encrypted using the key π:

$$T\ G\ E\ E\ M\ N\ E\ L\ N\ N\ T\ D\ R\ O\ E\ O\ A\ A\ H\ D\ O\ E\ T\ C\ S\ H\ A\ E\ I\ R\ L\ M$$

6. **[Pro]** (Shift Cipher Decryption) Please answer the following questions.

   (a) (5 pts) Please write a Python/MATLAB function for shift cipher decryption. This function should take the ciphertext (Y) and shift key (K) as inputs and output plaintext (x).

   (b) (5 pts) Use your function developed in part (a) to decrypt the provided cipher text file "*sampleFICT.txt*". Use the shift key, $K = 15$.
   i) Write the decrypted text to a file name "*#_$_shift_output.txt*", where "#" and "$" should be replaced with your first name and last name, respectively.
   ii) Print the 30^{th} to 39^{th} ciphertext characters in the file "*sampleFICT.txt*" and their corresponding plaintext.