**Nova Southeastern University**

**College of Computing and Engineering**

**ISEC 620 Applied Cryptography**

**Fall 2020**

**(August 17– December 6, 2020)**

Written Assignment #2

Due Date: October 4, 2020

Instructor: Dr. Junping Sun

1. What is the difference between a block cipher and stream cipher? (10 points)

**Stream = bit or byte at a time.**

**Block = who text block at a time.**

2. What is the difference between diffusion and confusion? (15 points)

In diffusion, the statistical structure of the plaintext is dissipated into long range statistics of

the ciphertext. This is achieved by having each plaintext digit a\_ect the value of many

ciphertext digits, which is equivalent to saying that each ciphertext digit is a\_ected by many

plaintext digits. Confusion seeks to make the relationship between the statistics of the

ciphertext and the value of the encryption key as complex as possible, again to thwart

attempts to discover the key. Thus, even if the attacker can get some handle on the statistics

of the ciphertext, the way in which the key was used to produce that ciphertext is so complex

as to make it di\_cult to deduce the key. This is achieved by the use of a complex substitution

3. Which parameters and design choices determine the actual algorithm of a Feistel cipher? (35 points)

**Block size: Larger block sizes mean greater security (all other things being**

**equal) but reduced encryption/decryption speed. Key size: Larger key size means greater**

**security but may decrease encryption/decryption speed. Number of rounds: The essence of**

**the Feistel cipher is that a single round o\_ers inadequate security but that multiple rounds**

**offer increasing security. Subkey generation algorithm: Greater complexity in this algorithm**

**should lead to greater diffculty of cryptanalysis. Round function: Again, greater complexity**

**generally means greater resistance to cryptanalysis. Fast software encryption/decryption: In**

**many cases, encryption is embedded in applications or utility functions in such a way as to**

**preclude a hardware implementation. Accordingly, the speed of execution of the algorithm**

**becomes a concern. Ease of analysis: Although we would like to make our algorithm as**

**di\_cult as possible to cryptanalyze, there is great bene\_t in making the algorithm easy to**

**analyze. That is, if the algorithm can be concisely and clearly explained, it is easier to**

**analyze that algorithm for cryptanalytic vulnerabilities and therefore develop a higher level**

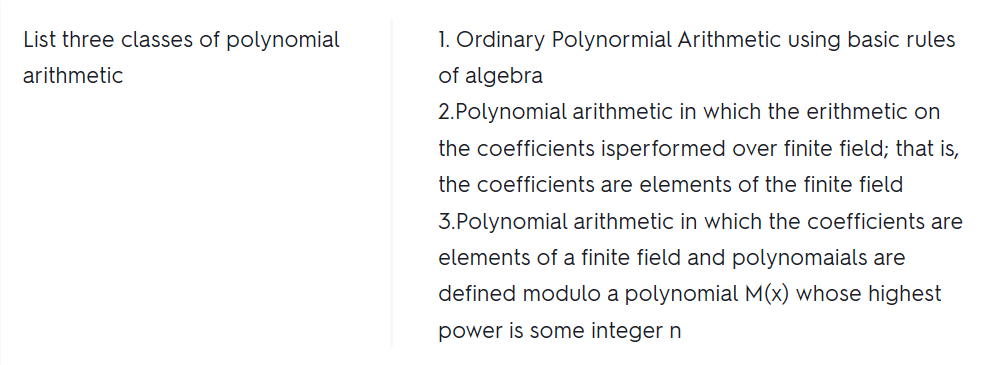
**of assurance as to its strength.**

4. What is the difference between differential and linear cryptanalysis? (10 points)

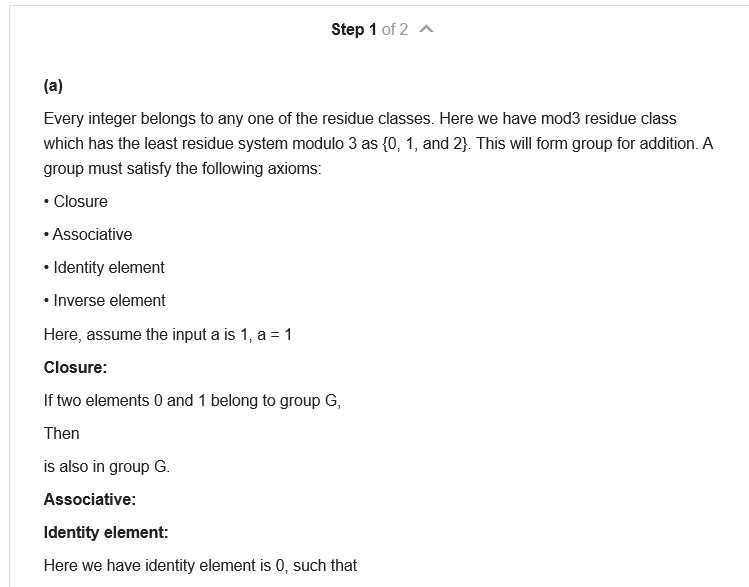
<https://techdifferences.net/difference-between-linear-and-differential-cryptanalysis/>

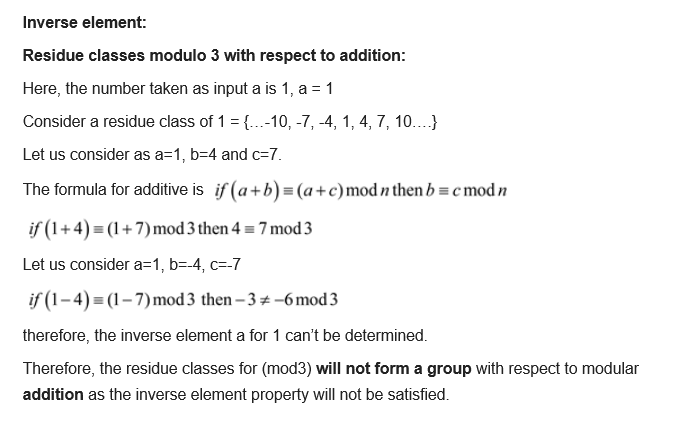
<https://vivadifferences.com/difference-between-linear-and-differential-cryptanalysis/>

5. List three classes of polynomial arithmetic. (15 points)

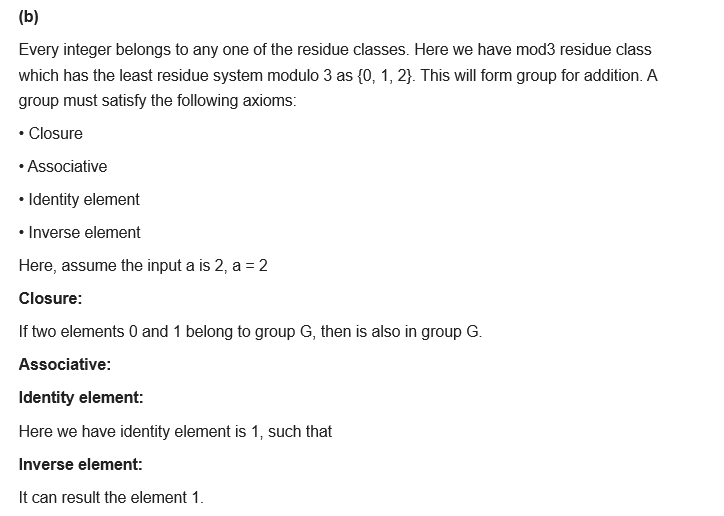


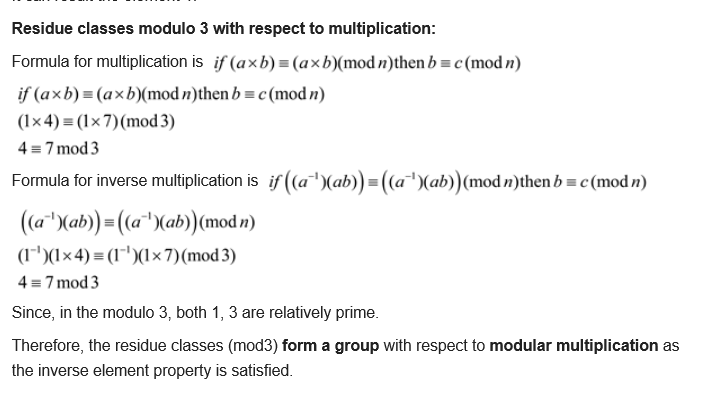
6. Does the set of residue classes modulo 3 form a group? (10 points)





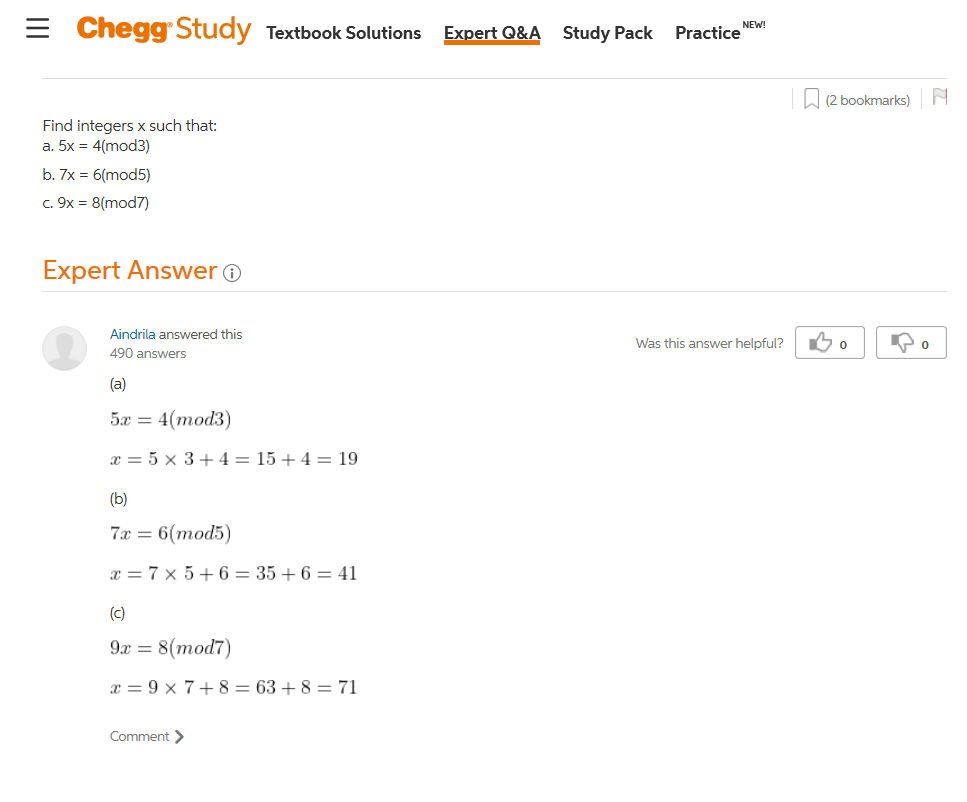
1. with respect to addition?
2. with respect to multiplication?



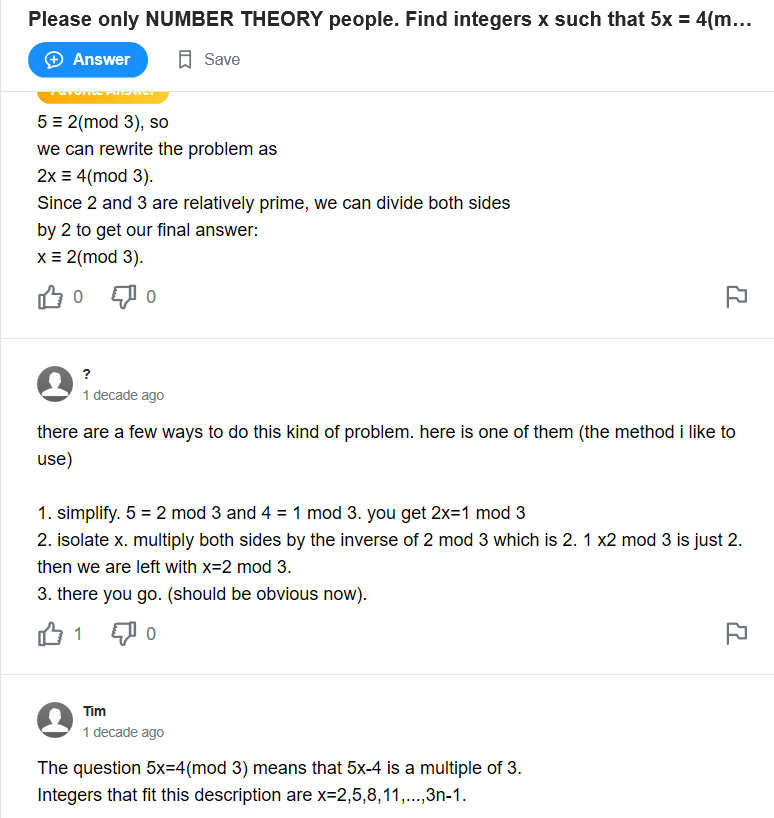


7. Find integers *x* such that:

1. 5*x* ≡ 4 (mod 3) (5 points)
2. 7*x* ≡ 6 (mod 5) (5 points)
3. 9*x* ≡ 8 (mod 7) (5 points)



**Try this too**

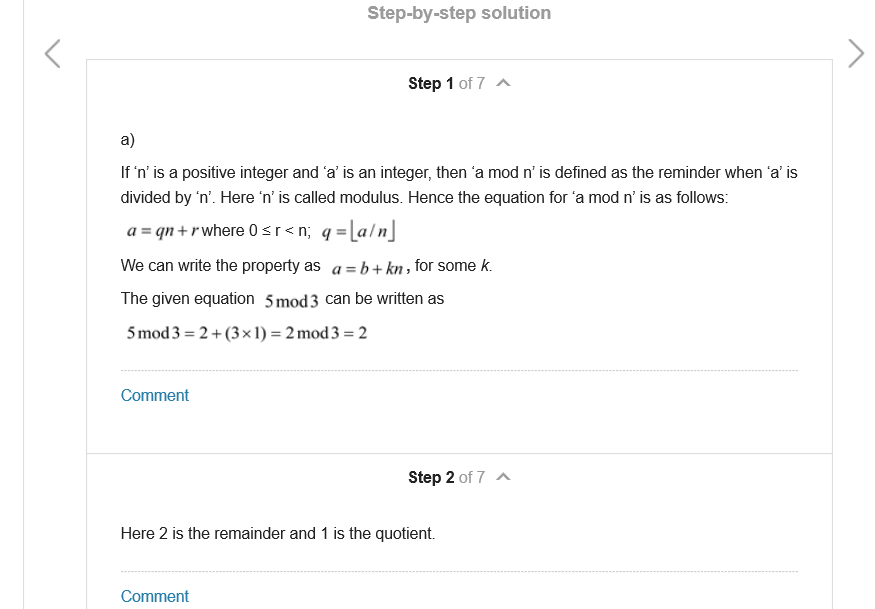


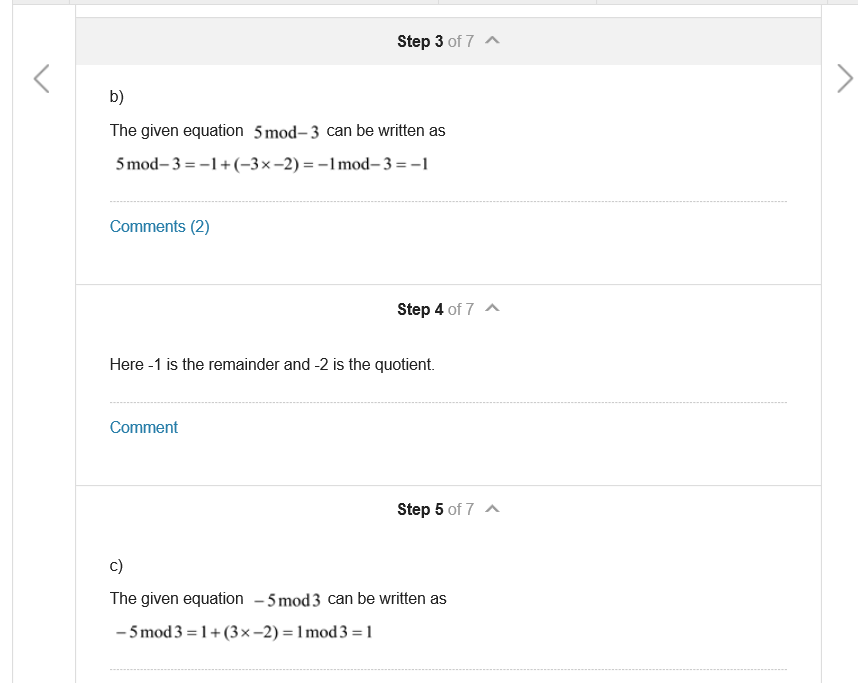
**ss**

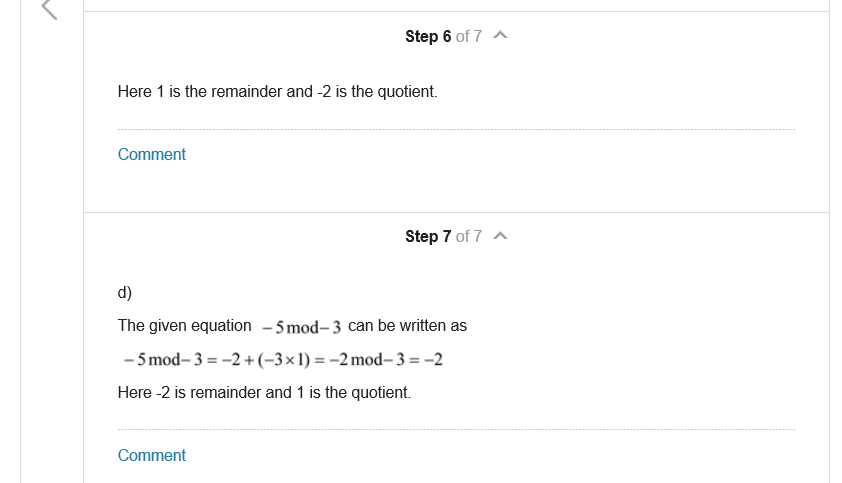
8. In this text we assume that the modulus is a positive integer. But the definition of the expression *a* mod *n* also makes perfect sense if *n* is negative. (20 points)

Determine the following:

1. 5 mod 3
2. 5 mod -3
3. -5 mod 3
4. -5 mod -3





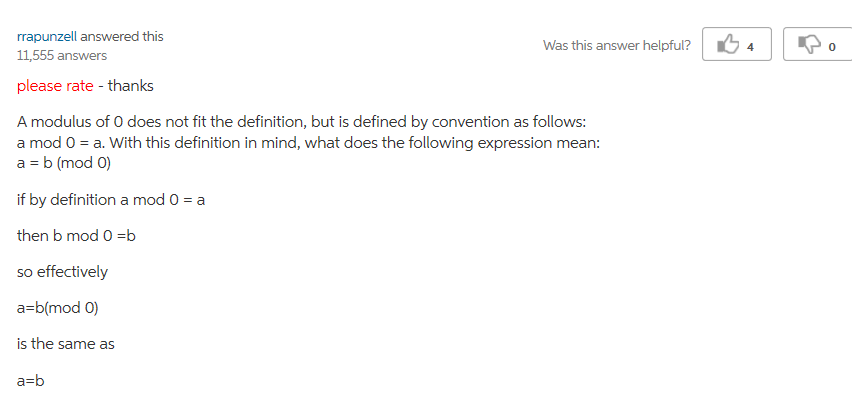


9. A modulus of 0 does not fit the definition, but is defined by convention as follows:

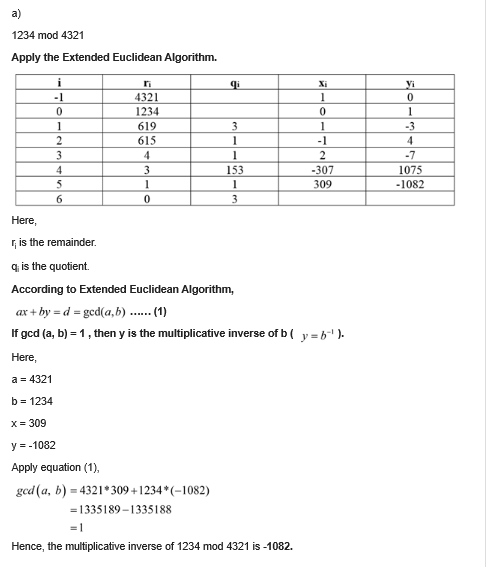
*a* mod 0 = *a*.

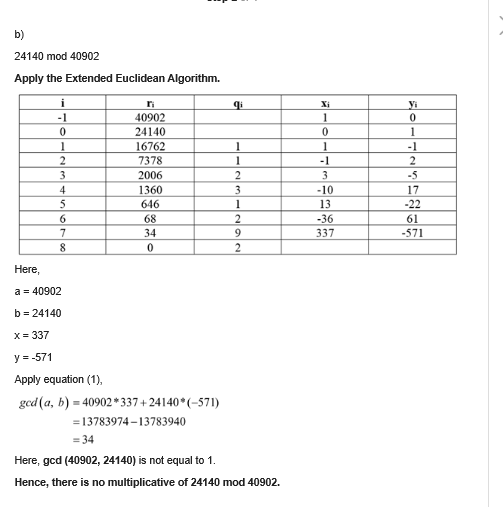
With this definition in mind, what does the following expression mean:

*a* ≡ *b* (mod 0) (10 points)

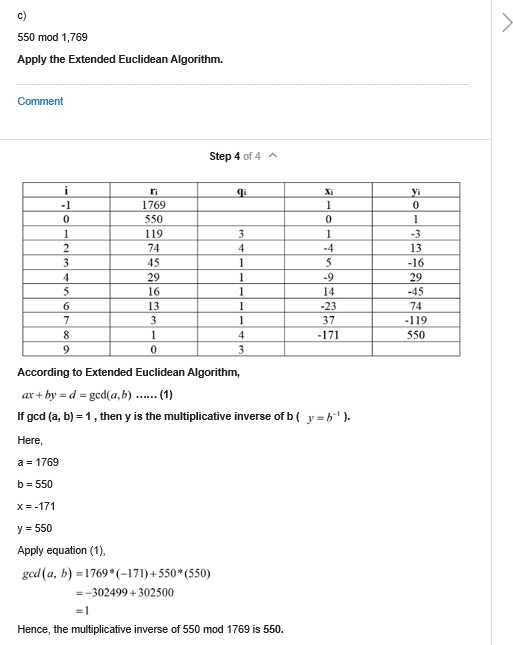


10. Using the extended Euclidean algorithm, and find the multiplicative inverse of

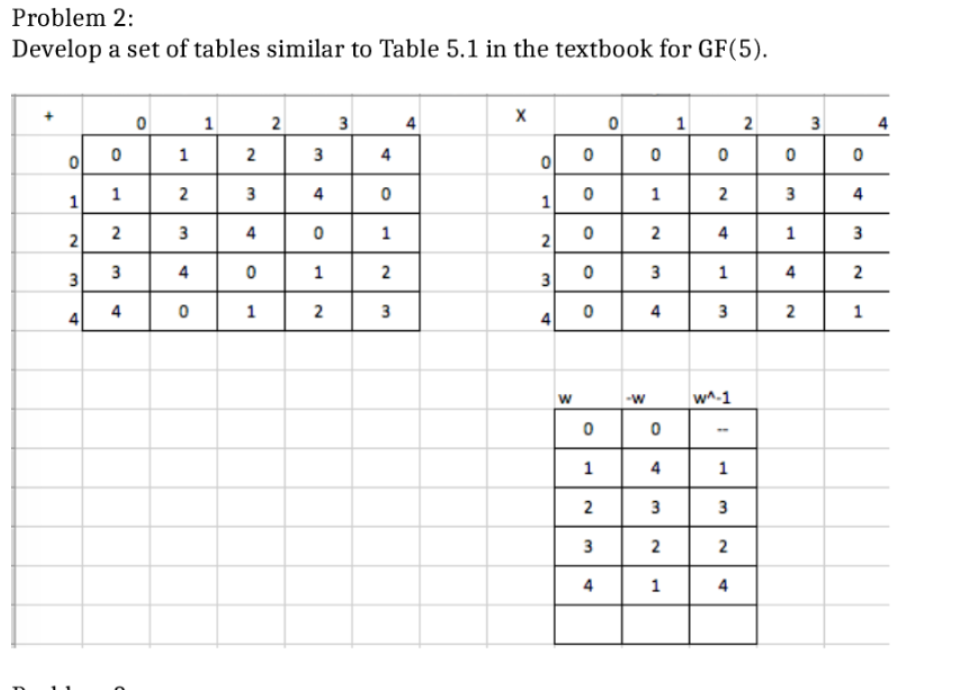
1. 1234 mod 4321 (5 points)
2. 
3. 24140 mod 40902 (5 points)

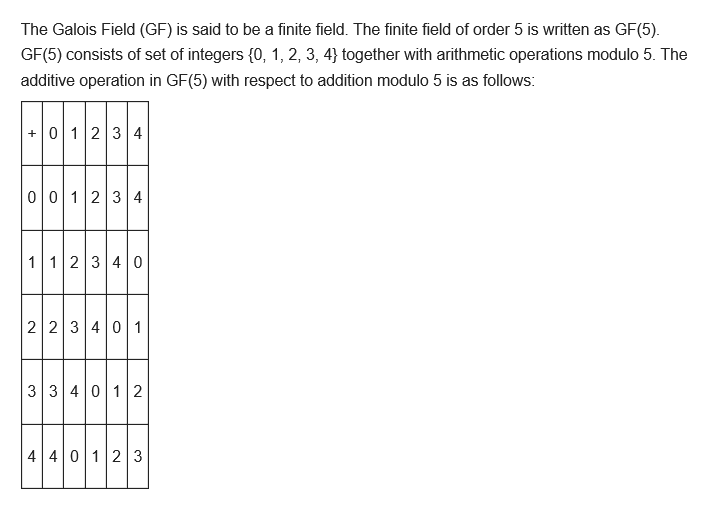


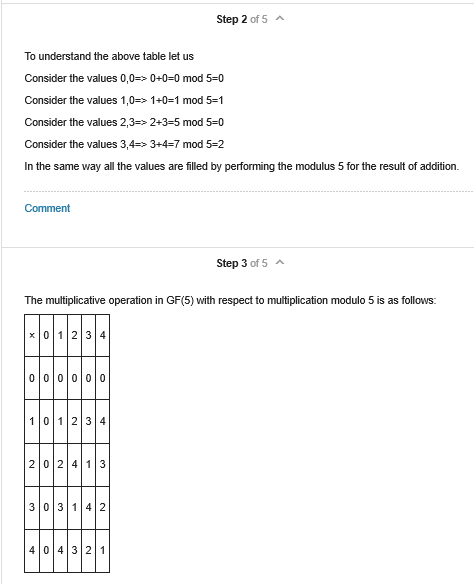
1. 550 mod 1769 (5 points)

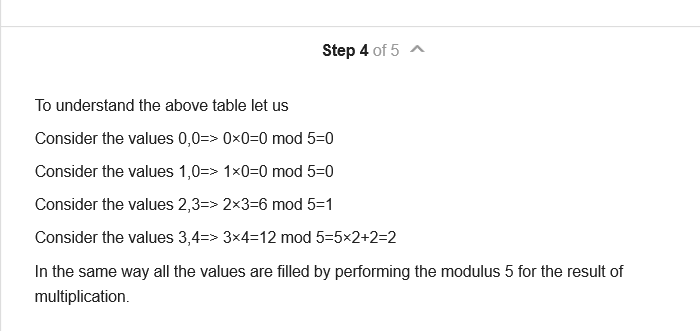


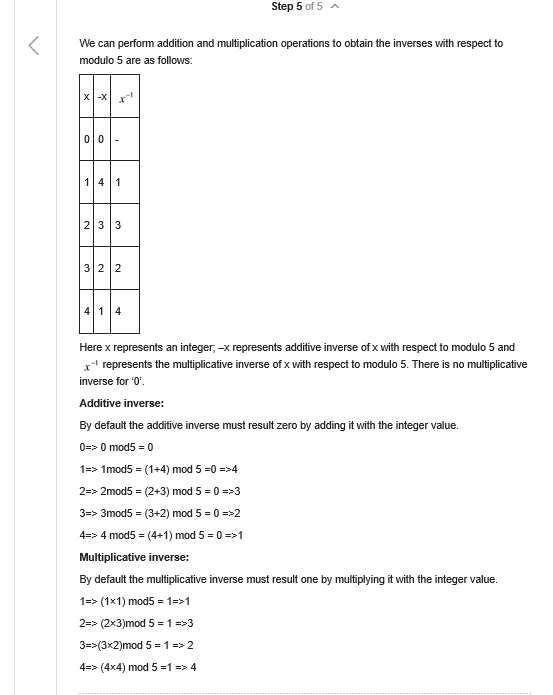
11. Develop a set of tables similar to Table 5.2 for GF(5). (20 points)



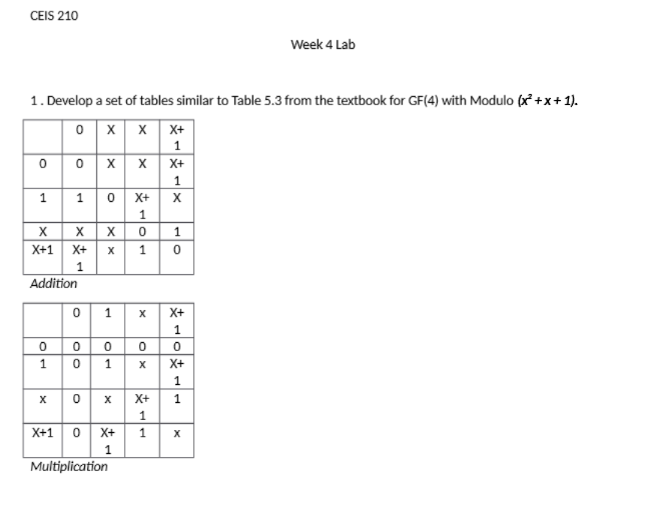


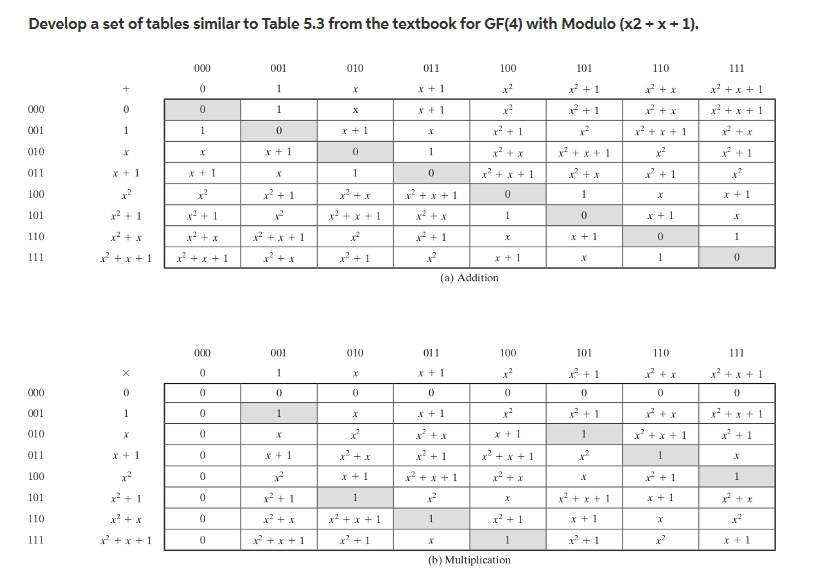






12. Develop a set of tables similar to Table 5.3 for GF(4) with *m*(*x*) = *x*2 + *x* +1 (20 points)





OTHER

