CS411 HW 2

Samuel Lee

24774

10/19/2019

1. For part a, the order of the group is 61 meaning that there can be a total number of 60 generators in Z, where generators are less than 61 and are co-prime to 61. Because 61 is a prime number, we can see cycle for some value (0 to 60) where the result of the discrete logarithm will result in a cycle. Two examples of the generators can be 2 & 6. For part b, using the Lagrange theorem, I found all possible subgroups in the group 61, and found a subgroup with order 5. The answer is : 1, 9, 20, 34, 58.
2. In order to find the answer, we first need to find the different variables. $\phi(n)$ where $n=p*q$ is a multiplicative function, meaning that $\phi(n) = \phi(p) * \phi(q)$, where $\phi(p) = p-1$ and $\phi(q) = q-1$. This function works because both p and q are prime numbers. Then I used a built-in function of python, pow(), to solve for m. The answer is : 3025624232311647114337757903685173495659956678495780877790008415934431140334807724330546889390094435679786549374287072364078639802603092317776014730871103745240338942225882488148569284312104218028021195525032789626303267205529411190014107098152321777301565858693092317773271396617297276351007405927094082041 6
3. For part a, the gcd(a,n) is 2, and because d is divisible by b, there may be two possible solutions. For part b, the gcd(a,n) is also 2, but because d is not divisible by b, there are no solutions for this linear congruence. For part c, the gcd(a,n)=1, meaning that there is a unique solution to the equation. The inverse of a is: 872089817864928642617281456 63, and the answer is: 32725272863917387420645850125 2
4. The functions in lfsr.py was used for this question. For the first equation, the result of the first period is equal to 2^L-1, which is 31. Therefore, it can be considered as a maximum period. For the second equation, the first period was equal to three, which was not equal to the maximum period value.
5. For this question, the FindPeriod and BM function was used to calculate the period of the bit sequence and the shortest LFSR. For all three of the examples(X1,X2,X3), the first period was 100 out of 100 length bit sequence, and the highest degree polynomials were 31. Furthermore, all the polynomials were the same with x^31+x^28+1. This means that they are unpredictable because it has the biggest period possible, considering the fact that the bit sequence were 100 bits long.