**Daniel Williamson**

**Project #7**

**4/8/16**

**CS 200**

Project Overview

Purpose:

The purpose of this project was to create a random number generator, using Linear Congruence. This is a very simple formula that takes any arbitrary integer as a "seed" and plugs it into an equation with some carefully-selected constants. The program is to read in a low number, and a high number and a count of how many random numbers the user wants. It should then display the random numbers and should be between the high and low numbers which were previously listed by the user.

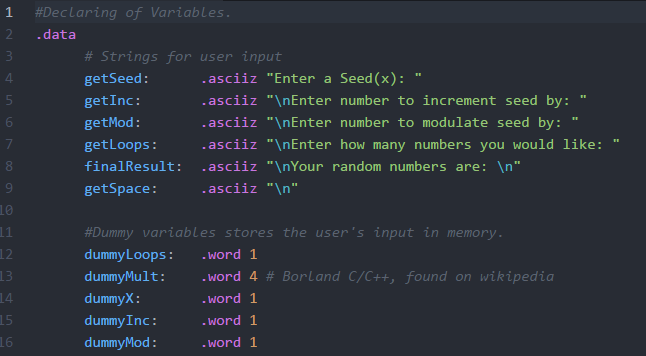
Approach:

To begin this project, I immediately went to the internet to gain a better understanding of how to program in Assembly. Also, how Linear Congruence works. I came across an algorithm for generating linear congruence, Xn+1 = (aXn + c) mod m. This is the calcuation I planned on fullfilling. Once I read up, I began to plan how the program should run. As per the structure of assembly I had to begin by declaring all my variables, strings included. I had to create some dummy variables to temporarily hold values until the user inputted them. After that, I started by asking for the users input and storing that into registers. Once I had all the input, I moved onto calculating the modulus and the recurrence relation formula while using a for loop to do it as many times and the user indicates.

Results

These are my results:

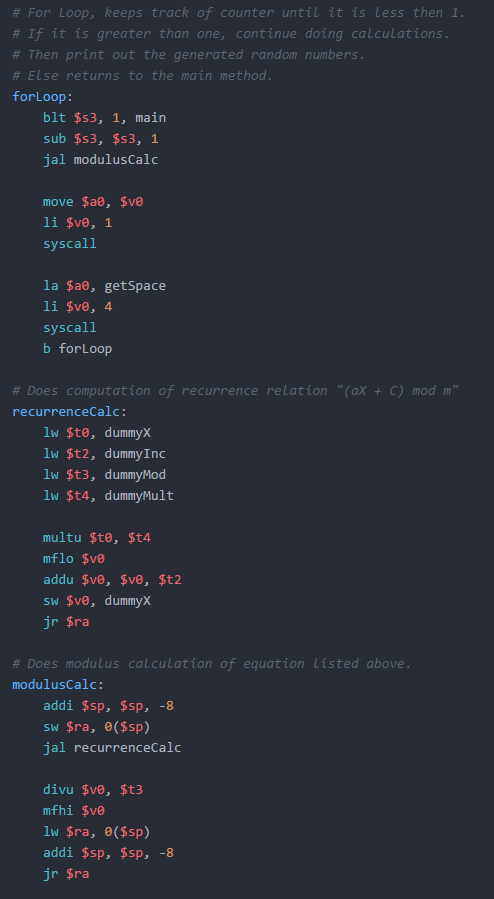
This is where I declared my variables/strings, the dummy variables are simply just temporary.



This is where we hold the values that we get from the getUserInput method.

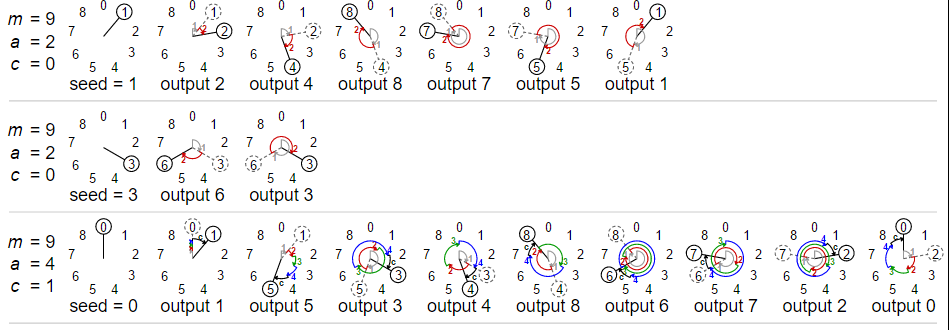


This is the forLoop method that loops through as many times as needed for how many numbers the user wanted. It does the recurrence relation calculation for each.

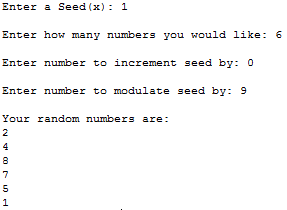


Testing:

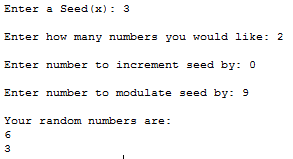
For my testing, I used this. Which was found on Wikipedia, along with my Linear Congruent algorithm.



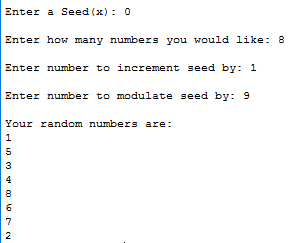
With the multiplier (a) set to 2, our seed at 1, our low (c, increment) at 0 and our high (m, modulate) at 9. We should get the random numbers of 2, 4, 8, 7, 5, and 1. Which we do:



With the multiplier (a) set to 2, our seed at 1, our low (c, increment) at 0 and our high (m, modulate) at 9. We should get the random numbers of 6 and 3. Which we do:



With the multiplier (a) set to 4, our seed at 0, our low (c, increment) at 1 and our high (m, modulate) at 9. We should get the random numbers of 1, 5, 3, 4, 8, 6, 7, and 2. Which we do:



Conclusion

In conclusion this is been the most difficult project yet. Simply because of the short amount of time getting to know how to even program in Assembly language. Not to mention trying to understand how Linear Congruency worked. However, once I was able to wrap my head around all of it, it become clear what was needed to be done. The hardest challenge I faced was just figuring out how to program in assembly.