Discrete Structures

2/19/2020

Homework 4

Congruencies

Section 4.4, Number 5  
Section 4.5, Number 5  
Section 4.6, Number 5

**A single sentence that explains what you learned or noticed.**

I learned about the Euclidean Algorithm and how it is implemented, as well as finding the inverse of a modulo.

**Section 4.4, Number 5**

Find an inverse of a modulo m for each of these pairs of relatively prime integers using the method followed in Example 2.

a) a =4, m =9

b) a =19, m =141

c) a =55, m =89

d) a =89, m =232

I am asked to find the inverse of a modulo m for specific numbers.

**References**

For this problem, my reference was slader.com, it provides the answer to the problem, but it also provides the solution steps which really helps me when I am struggling with a problem.

For the reference of the Euclidean Algorithm, I used Khan Academy.

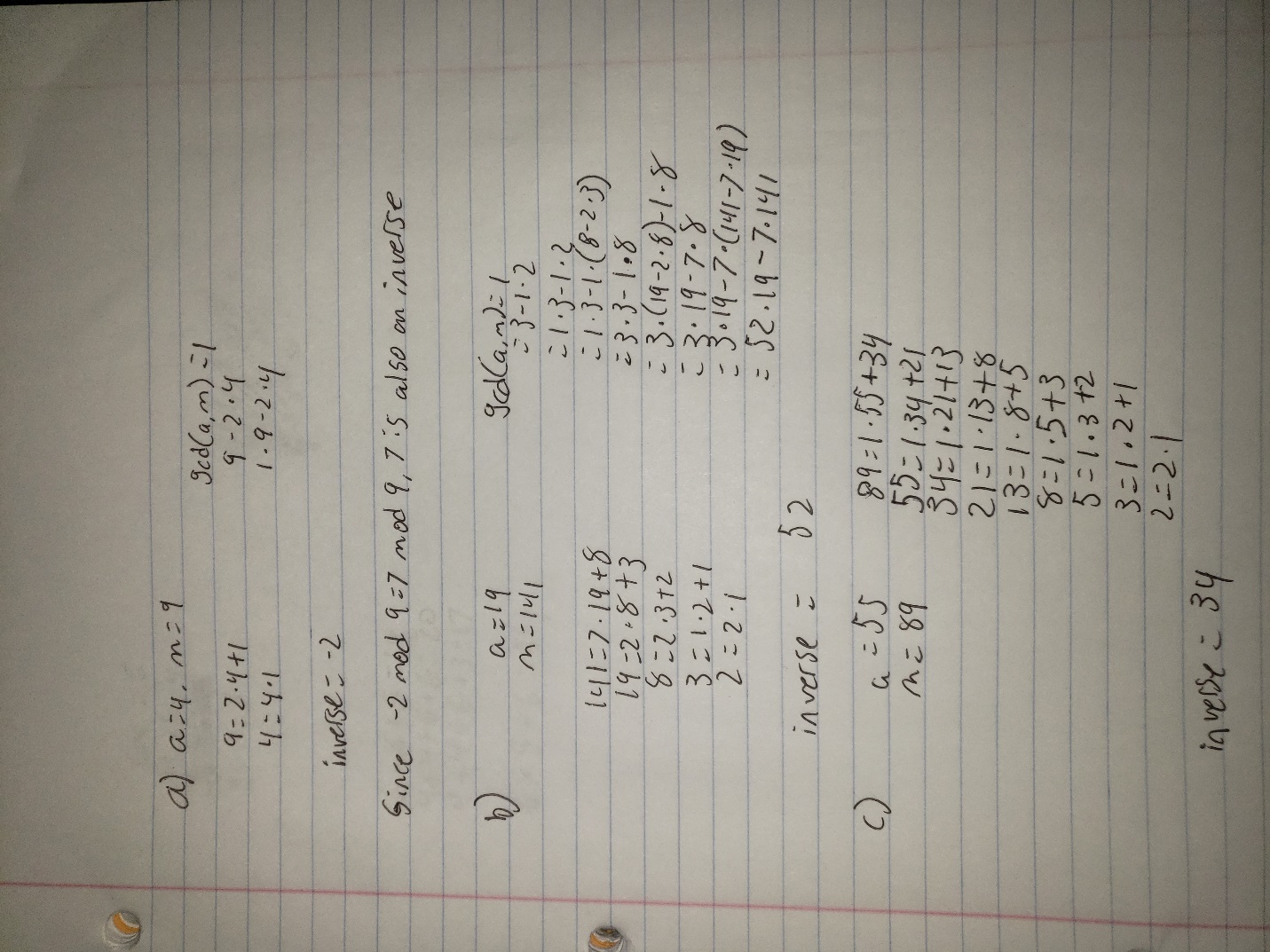
<https://www.slader.com/discussion/question/find-an-inverse-of-a-modulo-m-for-each-of-these-pairs-of-relatively-prime-integers/>

<https://www.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/the-euclidean-algorithm>

**Assumptions**

For this problem I to remind myself about what a modulo is. After that I assumed that finding the inverse would consist of using the Euclidean algorithm to find what else was needed.

**Calculations**



**Discussion of Solution**

For this solution, I applied the Euclidean Algorithm, then wrote the greatest common divisor as a multiple of a and m, then from there I took the coefficient of a, which is the inverse.

**Section 4.5, Number 5**

What sequence of pseudorandom numbers is generated using the linear congruential generator?

xn+1 = (3xn + 2) mod 13 with seed x0 =1?

In this problem I am asked to identify the sequence of numbers generated by the generator provided.

**References**

For this problem I also found the solution on Slader, It helped me mentally map out how the equation should be worked. I also didn’t fully understand how the generators themselves worked, so I used the second website to learn more about it.

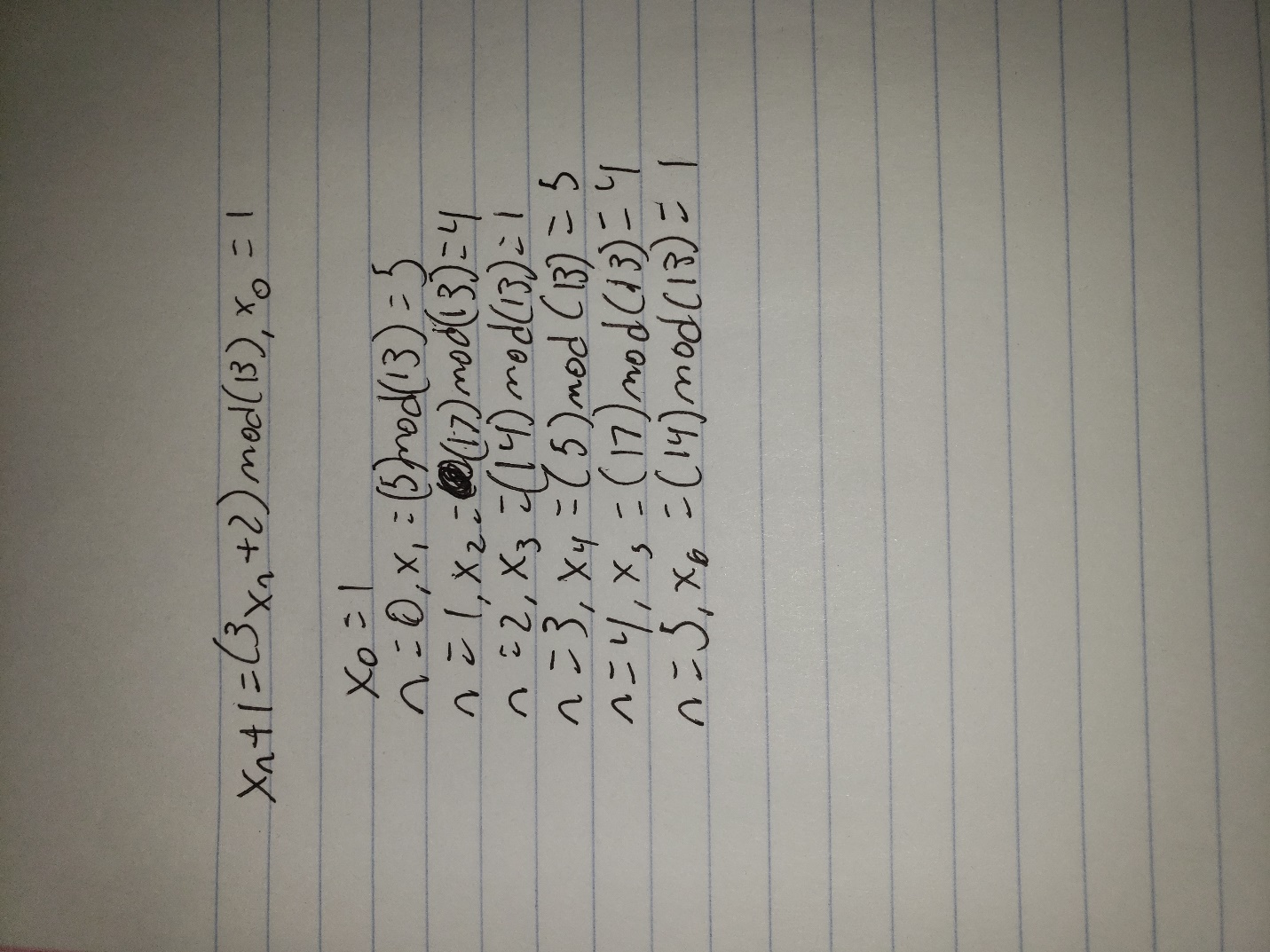
<https://www.slader.com/discussion/question/what-sequence-of-pseudorandom-numbers-is-generated-using-the-linear-congruential-generator-xn1-3xn-2/>

<https://www.geeksforgeeks.org/pseudo-random-number-generator-prng/>

**Assumptions**

From this being a random number generator, I knew what it would do in the end. However, I was not aware of the way that the seed would affect it and how intensive the formula for it is.

**Calculations**

****

**Discussion of Solution**

For this problem I first learned more about how pseudorandom number generators worked, and from there I was able to get the base idea on how to solve the problem. By using slader I was able to see the pattern and the way that problems like that are to be worked out. Once I understood it, I was able to finish the rest of the solution without much trouble.