Investigating whether the inputs of a Multiplicative Congruential Generator can be determined using the outputs

Yohwllo

March 10th 2024

Contents

1 Introduction

Ever since I was a young child the concept of random has amazed me. For randomness could at times not seem random, for example, number generators more often than not are far from random, instead they are psuedo random number generators, which are not truely random. These pesudo random number genrators are not truely random, but rather just a mathematical equation which is being done itteratively, and if the developer was forward thinking, it used a different seed every time too.
Now among random number generators there is a particularly common one called the Multiplicative Congruential Generator (MCG for short), it has been extensively used for various tasks that could require a lot of random numbers, that only need to be 'random enough'. For example creating test data, or for things such as dice rolling in games. There is also another type of random number genreator similar to it called the Linear Congruential Generator which is very similar in terms of how it functions.

Some asdclaisdm [2]
Department [1]
noi [3]

2 background

2.1 Random Number Generators

2.1.1 Multiplicitve Random Number Generator

Usually an MCG works based off of the equation $x_{i+1} = (a * x_i) \bmod m$. Where the next value is equal to the current value multiplied by a constant, and then its modulus is set as the remainder. [1]

2.1.2 Linear Congruential Generators

In contrast an LCG (Linear Congruential Generator) works in a very similar way, just adding a constant. Its equation looks like $x_{i+1} = (a * x_i + b) \bmod m$ [1]

References

[1] University Of Waterloo Math Department. generating random numbers. `https://wiki.math.uwaterloo.ca/statwiki/index.php?title=generating_Random_Numbers#Inverse_Transform_Method`, 2009.

[2] Michel Goossens, Frank Mittlebach, and Alexander Samarin. *The Latex Companion A*. Addison-Wesley, Reading, Massachusetts, 1993.

[3] noi. *the whack man*. nomanssky, reading Massachusetts, 2001.