Key Parameter Identification of Linear Congruential Method in Random Number Generation

Polash Kumar Guptho and Abul Mukid Md. Mukaddes
Department of Industrial and Production Engineering
Shahjalal University of Science and Technology
Sylhet 3114, Bangladesh
polashguptho@gmail.com,
mukaddes-ipe@sust.edu

Abstract

When analyzing real systems, collecting field data can be difficult. Therefore, many methods have been developed to generate artificial random numbers. One of the fundamental methods is the Linear Congruential Generation (LCG) method. It can generate random numbers based on the values of its parameters. This paper aims to identify the key parameter that has the highest impact on the performance of the LCG method, particularly in terms of the random number repetition period. To do this, the Design of Experiment (DOE) technique was used, and a model was developed using Minitab software. The experiment was conducted five times, and the average was taken for better results. The Python code of the LCG method was used to determine the random number repetition period. According to the results of the study, it was found that the parameter "m" had the highest impact on the performance of the LCG method, followed by "a", "c", and "Seed" respectively.

Keywords

Random number, LCG method, DOE, Key parameter, Python, random number repetition cycle, Minitab.

1. Introduction

Numerous external factors affect the systems under study and internal system component behaviors exhibit nondeterministic, or random, patterns. Therefore, it is required to reproduce the random effects that are present in the system to generate a simulation model that is reflective of the system under investigation. To incorporate random effects into consideration, random numbers are helpful. Using the stream of data gathered from the observation is one potential way to create the random effects that are present in the system. However, using field data has several drawbacks such as- limited in number, time-consuming, not applicable for non-existent systems, etc. Therefore, a method to artificially generate random data that satisfies the analyst's required criteria must be developed (Khoshnevis 1994). This algorithm or approach is known as a pseudo-random number generator. The most well-known pseudorandom number generator is the linear congruential method. Even though there are other alternatives, many users still prefer to use LCGs in their research works (Hermawan 2023). The quality of the random numbers produced by the LCG method is substantially impacted by the parameter values chosen (Averill and Dabid, 2003). However, no article explicitly demonstrates the size of the impact of each parameter on the effectiveness of the LCG method.

1.1 Linear Congruential Method (LCG)

The Linear Congruential method uses the following recursively evaluated equation with a random number generated at each iteration:

$$Z_i = (a*Z_{i-1}+c) \bmod m; \quad r_i = Z_i / m$$

where Z_0 is the seed. Parameters a, c, and m, as well as the seed, are nonnegative integers and must satisfy $0 < m$, $a < m$, $c < m$, and $Z_0 < m$ (Khoshnevis, 1994).

1.2 Objectives

This study aims to identify the key parameter of the LCG method that has the most impact on its performance so that users can carefully choose the value of the key parameter to get a satisfactory performance of the method on their specific task. The result should indicate the percentage of effects of each parameter on its performance, besides the impact of key parameters.

2. Literature Review

The LCG method is an important random number generation algorithm to generate random numbers and create randomization on the system under study. It has a wide range of applications, from analyzing a system to security purposes. Therefore, this paper focuses on identifying the key parameters of the LCG method. The literature related to the LCG method has been reviewed in this section.

Hermawan et al. (2023) designed an online-based exam using the Linear Congruent Method to randomize the question order and make the assessments quickly and precisely. Sun, T., & Li, S. (2023) gave the conditions to reach the full cycle for the linear congruence method to improve the method's performance. Aswathy et al. (2023) designed a lightweight Elliptic curve cryptography (ECC) based algorithm coupled with a linear congruential method to strengthen the security. in the cyber-physical system. Hashmi, M. A., & Tariq, N. (2023) used LCG method to provide a unique method to secure communication in smart cities. Abi Perbawa and Diana (2022) applied LCG method in the mathematics educational game to help students understand mathematics and provide a better learning experience. Gutierrez (2022) studied the linear congruential generator on elliptic curves based on lattice reduction techniques and analyzed some recent approaches. Faure et al. (2022) presented a method for generating a pseudorandom sequence (PRS) of numbers based on the linear congruential method. Elveny et al. (2020) designed a system using the LCG method to accumulate and transfer data from one device to another securely and efficiently. Panda and Ray (2019) proposed a new efficient PRBG method, i.e., "coupled-variable input LCG (CVLCG)," and its architecture for Pseudorandom Bit Generation. Juniawan et al. (2019) carried out a performance comparison testing in the form of speed testing based on the amount of randomized data between Linear Congruent Method (LCM) and Fisher-Yates Shuffle Algorithms. Vajargah and Asghari (2016) presented an efficient pseudo random number generator for cryptographic applications. Eichenauer and Lehn (1986) introduced a non-linear congruential pseudo random number generator and found that non-linear congruential pseudo-random number generator performed better than linear congruential generator in a simulation problem.

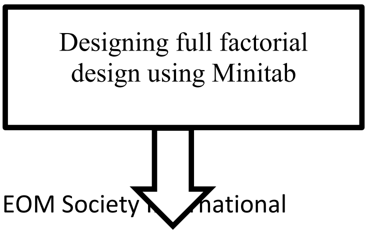
3. Methodology

This study focuses on identifying the key parameters of the LCG method. For identifying the impact of the parameters, some steps were followed, as shown in Figure 1.
Step 1: Designing a full factorial design: A full factorial design was created using the Minitab software for performing the Design of the Experiment. To do this, four values were randomly chosen for each parameter using an Excel function.
Step 2: Writing Python code and an Excel model of the LCG method: After developing the factorial design, the Python code and Excel model were developed for the LCG method to determine and verify the random number repetition period for each dataset respectively.

Step 3: Determining the random number repetition period: After developing the model, the random number repetition period for each dataset was determined.

Step 4: Analyzing the full factorial design: Afterwards, the full factorial design was performed in Minitab.

Step 5: Analyzing the results: As mentioned above, the design of the experiment was performed five times, which means steps 1 to 4 were iterated five times, and finally the results were interpreted.



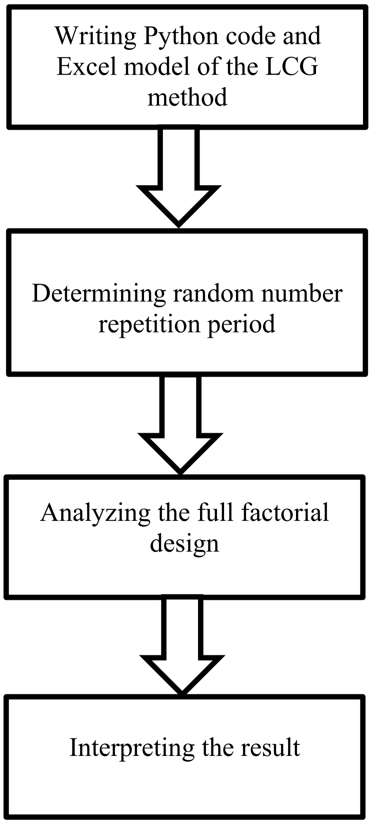

Writing Python code and Excel model of the LCG method
Determining random number repetition period
Analyzing the full factorial design
Interpreting the result

Figure 1**.** The methodology used for finding critical parameters of the LCG method.

3.1 Design of Experiment (DOE)

Design of Experiments (DOE) is a systematic and structured approach used in various fields, including science, engineering, manufacturing, and research, to plan, conduct, analyze, and interpret experiments to gain insights into the relationships between variables. DOE involves deliberately manipulating certain input factors (also known as independent variables or parameters) to observe their effects on one or more response variables.

Key steps of designing an experiment:

1. Identify the response variable and corresponding response factors: In this study, the response variable was the random number repetition period, and the factors were the parameters of the LCG method.
2. Determine the level of each factor: Four values or levels were taken for each factor to avoid complexity of having many experiments. There were 256 experiments for each full factorial design.
3. Then design the experiment based on the levels of factor: The experiment was designed automatically using the Minitab Software.
4. Then randomize the order of the experiment and calculate the response variable on each experiment: Randomization of the order of the experiment was done using the Minitab software. After that Python code and Excel model of the LCG method were used to calculate the response variable i.e., the random number repetition period on each experiment.

Then calculate the effect size of each factor: After determining the value of all response variables, the design was analyzed, and the effect size was determined using the Minitab software as shown in Figure 2.

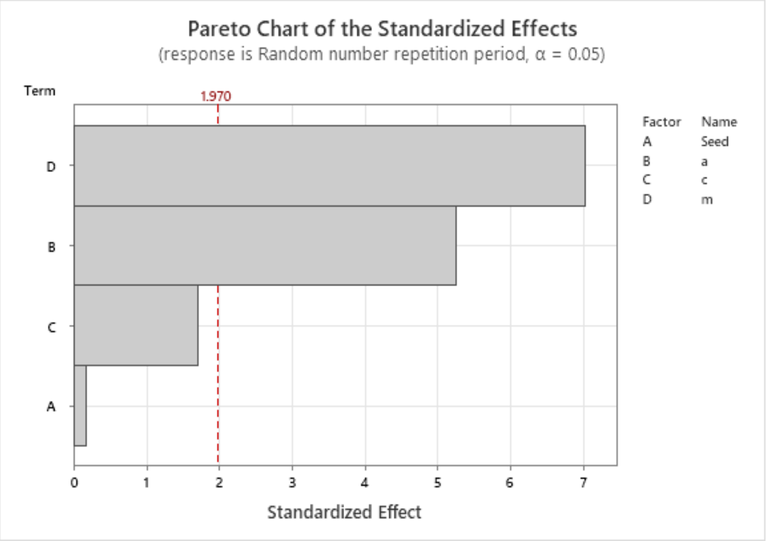


Figure 2. Effect of parameters on LCG method performance.

3.2 Materials

1. Python: Python language was used to write the LCG algorithm to generate random numbers and to determine the random number repetition period.
2. Excel: A mathematical model of the LCG method was developed in Excel to verify whether the Python code generates accurate random numbers. Additionally, the Excel "RANDBETWEEN ()" function was used for choosing the value of each factor.
3. Minitab: Minitab was used for performing the analysis part. The design of the experiment was conducted using Minitab software.

4. Results and Discussion

Design of Experiment was performed five times and the result for each experiment was determined as shown in Figure 3. The parameter 'm' had the largest impact on each experiment except the first experiment. On the contrary, 'Seed' has the least impact on the performance of the LCG method in each experiment. There were errors present on the results of the experiment for the following reason

Interaction between factors: As the effect size of each parameter was the main concern of this study, the interaction among the parameters was not considered, which caused errors.

Nonlinear relationships: In some cases, the increase of factor's value had inverse or no impact on the response variable, which caused errors.

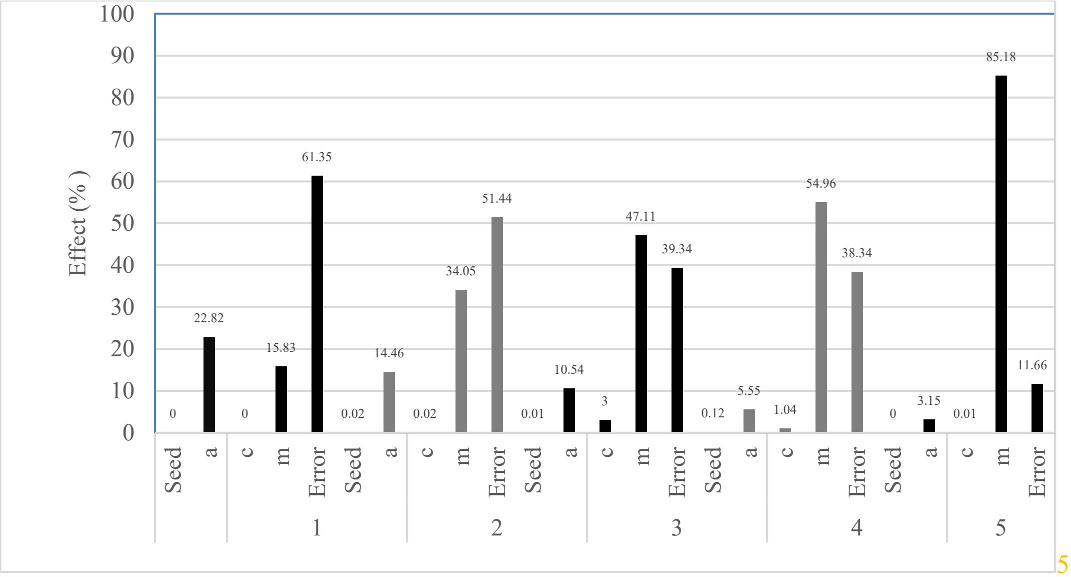


Figure 3. Effect of parameters of the LCG method in the five DOE

After analyzing and collecting the result of each experiment, the average contribution was calculated to find the key parameter of the LCG method as shown in Table 1. The cumulative result indicated that the parameter "m" has the largest impact on the random number repetition period (47.426%) than the parameters "a", "c" and "Seed" (11.304%, 0.814%, and 0.006%). From the experiment, it was found that "Seed" has the least impact on the random number repetition period in the LCG method.

Table 1. Results of the Key parameters of the LCG method.

Factor	**Average Contribution (%)**
Seed	0.006
a	11.304
c	0.814
m	47.426

5. Conclusion and Future Research

In this study, we have identified the key parameter of the Linear Congruential method in random number generation. The Design of the Experiment technique helps us to perform this analysis and get the results. Python code helps us to determine the repetition period of random numbers. The Excel model helps us to verify whether the repetition period is correct or not. The novelty of this study is finding the degree of effects of each parameter on the random number repetition period of the LCG method. The value of parameter 'm' should be chosen carefully as it has the largest impact on the method's performance. For further study, the number of design of experiment and level of factors may be enhanced to get more accurate results. The interaction between the factors could be analyzed to determine whether a certain pair of factors has a significant impact on its performance.

References

Hermawan, A., Susanti, W., Tendra, G., & Duha, Y., Application of the Linear Congruent Method In Online Exams in English. Digital Zone*: Jurnal Teknologi Informasi dan Komunikasi*, 14(1), 68-76, 2023.

Sun, T., & Li, S. (2023, March). Determination of full cycle condition by linear congruence method*. In Second International Conference on Electronic Information Engineering and Computer Communication (EIECC 2022)* (Vol.12594,pp.608-614).SPIE

Aswathy, R. H., & Malarvizhi, N., A design of lightweight ECC based cryptographic algorithm coupled with linear congruential method for resource constraint area in IoT. *Journal of Ambient Intelligence and HumanizedComputing*, 14(5),5097-5106, 2023.

Hashmi, M. A., & Tariq, N., An Efficient Substitution Box design with a chaotic logistic map and Linear Congruential Generator for secure communication in Smart cities. *EAI Endorsed Transactions on Smart Cities*, 7(1),2023.

Abi Perbawa, K., & Diana, D., Application of Linear Congruential Generator (LCG) Algorithm in Android Based Mathematics Education Game. *Jurnal Komputer, Informasi dan Teknologi (JKOMITEK)*, 2(1), 47-56, 2022.

Gutierrez, J., Attacking the linear congruential generator on elliptic curves via lattice techniques. *CryptographyandCommunications*,1-21,2022.

Faure, E., Fedorov, E., Myronets, I., & Sysoienko, S., Method for Generating Pseudorandom Sequence of PermutationsBasedonLinearCongruentialGenerator.*In CMIS* (pp.175-185), 2022.

Elveny, M., Syah, R., Jaya, I., & Affandi, I. (2020, June). Implementation of Linear Congruential Generator (LCG) Algorithm, Most Significant Bit (MSB) and Fibonacci Code in Compression and Security Messages Using Images. *In Journal of Physics: Conference Series* (Vol. 1566, No. 1, p. 012015). IOP Publishing.

Panda, A. K., & Ray, K. C., A coupled variable input LCG method and its VLSI architecture for pseudorandom bit generation. *IEEE transactions on instrumentation and measurement*, 69(4), 1011-1019, 2019.

Juniawan, F. P., Pradana, H. A., & Sylfania, D. Y. (2019, March). Performance comparison of Linear Congruent method and Fisher-Yates Shuffle for data randomization. *In Journal of Physics: Conference Series* (Vol. 1196, No.1,p.012035).IOPPublishing.

Vajargah, B. F., & Asghari, R., A novel pseudo-random number generator for cryptographic applications. *IndianJournalofScienceandTechnology*,9(6),1-5, 2016.

Eichenauer, J., & Lehn, J., A non-linear congruential pseudo random number generator. *Statistische Hefte*, 27(1),315-326, 1986.

Khoshnevis,B.(1994).Discretesystemssimulation.*McGraw-HillCollege.*

Averill M.Law, W.Dabid Kelton (2003). Simulation modeling and analysis. *McGraw-Hill Higher Education*

Biographies

Dr. Abul Mukid Md. Mukaddes is currently serving as a Professor at the Department of Industrial and Production Engineering at the Shahjalal University of Science and Technology (SUST), Sylhet, Bangladesh. He obtained his doctorate in engineering and master's degrees in engineering in computational mechanics from Kyushu University in Japan, respectively. He worked at Toyo University in Japan as a postdoctoral fellow. He graduated with a B.Sc. in engineering in the discipline of mechanical engineering. His current research focuses on system simulation, finite element analysis of engineering problems and information systems. He has published numerous articles in international journals and conference proceedings throughout his academic career.

Polash Kumar Guptho is an Undergraduate student at Shahjalal University of Science and Technology in Sylhet. He is currently working on a thesis under the supervision of Professor Dr. Abul Mukid Md. Mukaddes. His research interests are Operations Research, Machine Learning & Simulation.