SCIENTIFIC PUBLICATIONS OF THE STATE UNIVERSITY OF NOVI PAZAR
SER. A: APPL. MATH. INFORM. AND MECH. vol. 15, 2, 2023, 87–95

Extension of Linear Congruential Generator

Atif Avdović

Abstract: Random number generation is a significant research topic, even though there have already been a lot of papers published about it. Particularly detailed research has been made about the Linear Congruent Generator (LCG), which is still the most frequently used one. Research into the LCG has lead to the results in this paper in form of a new, extended LCG model. We have shown that the extended model has all the necessary features of randomness, but still a significantly larger period than the standard LCG.

Keywords: extension, linear congruential generator, period, modulus, randomness, number theory

1 Introduction

The Linear congruential generator (LCG), often referred to as a simple linear congruential linear generator or Lehmer's congruential generator, introduced by Lehmer [14], is shown to be the most commonly used random number generator [4], [8] (p. 11). This is due to distinctive features of LCG such as simplicity, programmability, and speed. The importance of these characteristics is discussed by Devroye in his highly important textbook [3]. However, what seemed to be the issue was the period length, which was thus extensively discussed and researched. However, choice of the multiplicator has been discussed more than choice of the modulus.

Knuth has analyzed LCG and obtained results that show the optimal modulus for the multiplicator 2^k+1 is a prime number even though the modulus $2^p(p>k)$ yields the fastest generating [13] (pp. 12-15). Some issues concerning this choice of multiplicator and modulus are discussed in [17]. Namely, Park and Muller [17] have stated that LCG with modulus $2^{31}-1$ and multiplicator 16807 should be taken as a minimal standard in terms of period and randomness. However, Tang [19] discusses that good randomness and period properties of LCG are obtained for the modulus values of the ten largest prime numbers smaller than 2^{31}. Moreover, Fishman and Moore [5] provided a list of 414 optimal multiplicators for this modulus. Park and Muller [17] found that the actual number of those multipliers is 410 and the number 414 in the original paper is stated due to the error.

Manuscript received August 5, 2023; accepted November 7, 2023.

Department of sciences and mathematics, State university of Novi Pazar, Vuka Karadžića 9, 36300 Novi Pazar, Serbia, aavdovic@np.ac.rs

Also, modulus 2^{32} is used due to the simplicity of generating numbers. This modulus has an additional advantage because of odd increments and multiplicators equivalent to $\pm 3 \mathrm{mod} 8$ it reaches maximal period [15]. Fishman [6] gave an exhaustive analysis of this modulus.

Due to the larger period necessity and better computer performance, as well as the need for better quality of generated numbers, the improvement of LCG performance has been attempted via modulus increase from the usually used modulus of $2^{31}-1$ to the larger ones, such as $2^{61}-1$, and similar variants [20].

Theoretical background for this generator was not established from the beginning, but that issue has later been consolidated and widely discussed in many papers [7] as well as textbooks [13] (pp. 16-21). According to Park and Muller [17] the most complete theory is developed for multiplicative and mixed LCGs.

Though well researched for a long time, random number generation is in no way a closed topic due to the constant need for modelling big data because of exponentially growing number of application areas. This can be seen in recent textbooks such as [16]. New random number generators, whether they are based on modular reduction or not [9] are still developed, discussed, tested and compared [10] to other known generators. In this sense the present paper offers an important improvement of a widely used and researched random number generator that is still of interest for application as well as further scientific research such as control charts performance analysis [11, 12], goodness-of-fit tests power analysis [1, 2], probabilistic topic modelling [18] etc.

In this paper, an extension of the LCG that provides random number sequences of significantly larger periods is introduced and some of its properties are also given. The following section provides preliminary facts about the LCG. Section 3 contains some results concerning the extension of LCG and the increase of the period length. In Section 4, concluding remarks are given.

2 Preliminaries

Definition 2.1. *The Linear Congruential Generator is given by the equation*

$$X_n = (aX_{n-1} + c) \mathrm{mod} m \tag{1}$$

where a, c, m, n, X_0 are all positive integers, and are called the multiplicator, the increment, the modulus and the seed respectively. Based on the module properties, we can write $n, m \in \mathbb{N}; a, c \in \{1, 2, ..., m-1\}; X_i \in \{0, 1, 2, ..., m-1\}; i = 1, 2, ...$ When $c = 0$ LCG is called the Multiplicative Gongruential Generator.

It is important to state the following theorem that Knuth [13] (p. 17) has elaborated on in detail.

Theorem 2.1. *The LCG given with (1) and with seed X_0 has a period length of m if and only if c is relatively prime to m, $a-1$ is a multiple of every prime divider of m and $a-1$ is multiple of 4 when m is multiple of 4.*

The following notions are of importance for multiplicative LCG and its period. Gentle has offered sources for further reading [8].

Definition 2.2. *Number a such that in equation*

$$a^k = 1 \bmod m$$

$k = \phi(m)$ holds, where ϕ is Euler's function (the number of primes less than m), is called primitive root modulo m.

Theorem 2.2. ***(Euler-Fermat theorem)*** *If a and m are relatively prime, then*

$$a^{\phi(m)} = 1 \bmod m$$

holds.

Lemma 2.1. *If for multiplicative LCG $X_n = (aX_{n-1}) \bmod m$ the equation $a^k = 1 \bmod m$ holds, then this generator's period length is not larger than k.*

Remark 2.1. Trivial, but an important fact that follows is that for prime m the number of primitive roots modulo m is $\phi(m-1)$ and if a is such a number, multiplicative LCG can reach its maximal period $\phi(m)$.

3 Results

Definition 3.1. *LCG with the Extension is the generator given with the recurrent formula*

$$X_n = \Upsilon(aX_{n-1} + c, k_{X_{n-1}}) \bmod m$$

where $\Upsilon : \mathbb{N}^2 \to \mathbb{N}$ is a linear function, and $k_{X_{n-1}} = \sum_{i=1}^{n-1} I(X_i = X_{n-1})$, for I being the event indicator, i.e. the random variable that equals 1 when the argument event is true. Value $k_{X_{n-1}}$ is called ***the extension*** *of the generator.*

In this paper, some cases of LCG with the Extension and its properties are discussed. The function Υ represents a linear function where X_i is its argument, and $k_{X_{n-1}}$ is used to modify the LCG recurrent formula, simply by taking a count of the number of occurrences of generated numbers. The choice of the function Υ is also discussed.

Case 1. LCG with the additive Extension is given with the recurrent formula:

$$X_n \equiv (aX_{n-1} + k_{X_{n-1}}c) \bmod m$$

Case 2. LCG with the multiplicative Extension is given with the recurrent formula

$$X_n \equiv (k_{X_{n-1}}aX_{n-1} + c) \bmod m$$

Case 3. Extended LCG is given with the recurrent formula

$$X_n \equiv k_{X_{n-1}}(aX_{n-1} + c) \bmod m$$

Conditions $a \neq 0$ and $c \neq 0$ are set because otherwise, situations of no interest occur. For instance, taking $c = 0$, in the first case, the generator becomes multiplicative congruential generator. In the second and the third case, once $X_i = 0; i = 0, 1, 2, ...;$ the $X_{i+k} = 0; k \in \mathbb{N}$ holds. For $a = 1$ and $c = 1$, generated numbers cannot be used as random numbers because the distribution of the obtained sample usually is not a uniform one [13] (pp. 16-17).

Theorem 3.1. *Let X_{n-1}, X_n and X_{n+1} be the numbers generated using LCG with the additive or the multiplicative Extension or using the Extended LCG. The expression*

$$X_{n-1} = X_n = X_{n+1}$$

is false for any positive integer n and for any choice of generator parameters.

Proof. LCG with additive extension
Assuming the opposite implies that there is a positive integer n_0 such that $X_{n_0-1} = X_{n_0} = X_{n_0+1}$. Then

$$X_{n_0} \equiv (aX_{n_0-1} + k_{X_{n_0-1}}c)\text{mod}m \equiv X_{n_0-1}$$

and

$$X_{n_0+1} \equiv (aX_{n_0} + k_{X_{n_0}}c)\text{mod}m \equiv (aX_{n_0-1} + (k_{X_{n_0-1}} + 1)c)\text{mod}m \equiv X_{n_0-1}$$

Hence, $c = 0$, which is impossible because $c \in \{1, 2, ..., m-1\}$.

LCG with multiplicative extension
Assuming the opposite implies that there is a positive integer n_0 such that $X_{n_0-1} = X_{n_0} = X_{n_0+1}$. Then

$$X_{n_0} \equiv (ak_{X_{n_0-1}}X_{n_0-1} + c)\text{mod}m \equiv X_{n_0-1}$$

and

$$X_{n_0+1} \equiv (ak_{X_{n_0}}X_{n_0} + c)\text{mod}m \equiv (a(k_{X_{n_0-1}} + 1)X_{n_0-1} + c)\text{mod}m \equiv X_{n_0-1}$$

Hence, $a = 0$, which is impossible because $a \in \{1, 2, ..., m-1\}$.

Extended LCG
If X_{n-1}, X_n and X_{n+1} are generated using the Extended LCG and if $X_{n-1} = X_n = X_{n+1}$ is true for some positive integer n, then

$$X_{n-1} \equiv k_{X_{n-1}}(aX_{n-1} + c)\text{mod}m$$

and

$$X_{n-1} \equiv (k_{X_{n-1}} + 1)(aX_{n-1} + c)\text{mod}m$$

Subtracting these equivalences implies

$$(aX_{n-1} + c)\text{mod}m \equiv 0$$

Hence there are two possibilities. First that $X_{n-1} = 0 \wedge c = 0$, $a = 0 \wedge c = 0$, $X_{n-1} = 0 \wedge a = 0 \wedge c = 0$ is true which is impossible because on the definition of the Extended LCG. Another possibility is that

$$aX_{n-1} + c = qm; q \in \mathbb{N} \Rightarrow X_{n-1} = \frac{qm - c}{a} \in \{1, ..., m-1\}$$

(if $X_{n-1} = 0$ then $c = 0$ again). In that case,

$$X_n = 0 \equiv k_{X_{n-1}}(a\frac{qm-c}{a} + c)\text{mod}m \equiv 0$$

which means $X_{n-1} \neq X_n$, so the contradiction to the initial assumption occurs. Therefore, the statement of the theorem is proven. □

Theorem 3.2. *Let X and Y be the numbers generated respectively using LCG with the additive Extension, and let* $k_X = \min\{d \in \mathbb{N} | (aX + dc)\text{mod}m \equiv Y\}$. *Then* $(X_{n-1}, X_n) = (X, Y)$ *is true for some positive integer n if and only if* $k_{X_{n-1}} = lm + k_X; l \in \mathbb{N}_0$. *If* $k_{X_{n-1}} > k_X$*, then l is a positive integer. The same holds for LCG with the multiplicative Extension where* $k_X = \min\{d \in \mathbb{N} | (daX + c)\text{mod}m \equiv Y\}$*, and the Extended LCG where* $k_X = \min\{d \in \mathbb{N} | d(aX + c)\text{mod}m \equiv Y\}$.

Proof. LCG with additive extension:
(⇒): Let $(X_{n-1}, X_n) = (X, Y)$. Then

$$X_n \equiv (aX_{n-1} + k_{X_{n-1}}c)\text{mod}m \Leftrightarrow Y \equiv (aX + k_{X_{n-1}}c)\text{mod}m$$

Since $k_{X_{n-1}} \in \mathbb{N}$, there are numbers $l \in \mathbb{N}_0$ and $r \in \{0, 1, ..., m-1\}$ such that $k_{X_{n-1}} = lm + r$. Hence,

$$Y \equiv (aX + (lm + r)c)\text{mod}m \equiv (aX + rc)\text{mod}m \tag{2}$$

There is no positive integer smaller than r which can satisfy (2), so $k_X = r$. Obviously, if $k_{X_{n-1}} > k_X$, then $l \in \mathbb{N}$.
(⇐): Let $X_{n-1} = X$ for some positive integer n, and let $k_{X_{n-1}} = lm + k_X; l \in \mathbb{N}_0$. Then

$$X_n \equiv (aX_{n-1} + k_{X_{n-1}}c)\text{mod}m \equiv (aX + (lm + k_X)c)\text{mod}m \equiv (aX + k_Xc)\text{mod}m \equiv Y$$

Hence, because X_n and Y are generated with LCG with the additive Extension, $X_n = Y$, i.e. $(X_{n-1}, X_n) = (X, Y)$.

LCG with multiplicative extension
(⇒): Let $(X_{n-1}, X_n) = (X, Y)$. Then

$$X_n \equiv (ak_{X_{n-1}}X_{n-1} + c)\text{mod}m \Leftrightarrow Y \equiv (ak_{X_{n-1}}X + c)\text{mod}m$$

Since $k_{X_{n-1}} \in \mathbb{N}$ there are numbers $l \in \mathbb{N}_0$ and $r \in \{0, 1, ..., m-1\}$ such that $k_{X_{n-1}} = lm + r$. Hence,

$$Y \equiv (a(lm + r)X + c)\text{mod}m \equiv (arX + c)\text{mod}m \tag{3}$$

There is no positive integer smaller than r which can satisfy (3), so $k_X = r$. Obviously, if $k_{X_{n-1}} > k_X$, then $l \in \mathbb{N}$.
(⇐): Let $X_{n-1} = X$ for some positive integer n, and let $k_{X_{n-1}} = lm + k_X; l \in \mathbb{N}_0$. Then

$$X_n \equiv (ak_{X_{n-1}}X_{n-1} + c)\text{mod}m \equiv (a(lm + k_X)X + c)\text{mod}m \equiv (ak_XX + c)\text{mod}m \equiv Y$$

Hence, because X_n and Y are generated with LCG with the multiplicative Extension, $X_n = Y$, i.e. $(X_{n-1}, X_n) = (X, Y)$.

Extended LCG

($\Rightarrow$): Let $(X_{n-1}, X_n) = (X, Y)$. Then

$$X_n \equiv k_{X_{n-1}}(aX_{n-1} + c)\text{mod}m \Leftrightarrow Y \equiv k_{X_{n-1}}(aX + c)\text{mod}m$$

Since $k_{X_{n-1}} \in \mathbb{N}$ there are numbers $l \in \mathbb{N}_0$ and $r \in \{0, 1, ..., m-1\}$ such that $k_{X_{n-1}} = lm + r$. Hence,

$$Y \equiv (lm + r)(aX + c)\text{mod}m \equiv r(aX + c)\text{mod}m \tag{4}$$

There is no positive integer smaller than r which can satisfy (4), so $k_X = r$. Obviously, if $k_{X_{n-1}} > k_X$, then $l \in \mathbb{N}$.

($\Leftarrow$): Let $X_{n-1} = X$ for some positive integer n, and let $k_{X_{n-1}} = lm + k_X; l \in \mathbb{N}_0$. Then

$$X_n \equiv k_{X_{n-1}}(aX_{n-1} + c)\text{mod}m \equiv (lm + k_X)(aX + c)\text{mod}m \equiv k_X(aX + c)\text{mod}m \equiv Y$$

Hence, because X_n and Y are generated with LCG with the multiplicative Extension, $X_n = Y$, i.e. $(X_{n-1}, X_n) = (X, Y)$. □

Remark 3.1. The number k_X belongs to the set $\{0, 1, ..., m-1\}$ because otherwise it could be written as $k_X = lm + r; l \in \mathbb{N}; r \in \{0, 1, ..., m-1\}$ and then

$$Y \equiv (aX + k_X c)\text{mod}m \equiv (aX + (lm + r)c)\text{mod}m \equiv (aX + rc)\text{mod}m$$

would hold, which means $r < k_X$ where k_X is minimal such a value. That is impossible. The same goes for Case 2 and Case 3 of the generator.

Theorems 3.1 and 3.2 show that the extension LCG generates numbers with no lose of property of randomness.

The following theorem gives insight into the extension's impact on the period length of LCG.

Theorem 3.3. *Let $p \neq 2$ be a prime, c relatively prime to p^k and*

$$h_{x_n} = \begin{cases} k_{X_n}, & k_{X_n} \neq p \\ k_{X_n} + 1, & k_{X_n} = p \end{cases}.$$

Generator given with

$$X_{n+1} = ((p^l + 1)X_n + h_{X_n} c)\text{mod}p^k, \tag{5}$$

for $l \in \{1, ..., k-1\}, k \in \mathbb{N}$ has minimal period legnth $p^{ks} + d_i$, and maximal period length $\sum_{i=1}^{v}(p^{ks} + d_i)$, where $s = \sum_{j=1}^{m-1} I(j \neq p^l, l \in \{1, 2, ..., p^k - 1\})$, d_i is period length of generator given with $X_{n+1} = (p^l + 1)X_n\text{mod}p^k$ and v is the number of its different variates generated last before reaching its period for differents seeds $X_0 = i, i = 0, ..., p^k - 1$ (v is not larger than p^k).

Proof. For $a = p^l + 1$ number $a - 1 = p^l$ is a multiple of $m = p^k$. Since c is relatively prime to p^k, all of the numbers $(j \cdot c)\text{mod}p^k, j = 1,...,p^k - 1, j \neq p^l, l = 1,...,p^{k-1}$ are relatively prime to p^k, and thereby so are the numbers $(h_{X_n} \cdot c)\text{mod}m$. Also, the condition $p \neq 2$ indicates both $a - 1$ and p^k are not multiples of 4. Thus, generators obtained from (5) when h_{X_n} is fixed, satisfy the conditions of Theorem 2.1. Hence, each one of them reaches its maximal possible period of $m = p^k$ for any seed. Generator (5) is constructed by these s generators performing respectively. After each of these generators reaches a full period of p^k, $h_{X_n} = p^k$ is reached, thus the following numbers to be generated are the result of generator $X_{n+1} = (p^l + 1)X_n\text{mod}p^k$ which has period denoted with d_i for seed $X_0 = i, i \in \{0, 1, ..., p^k - 1\}$. Hence, generator (5) has period length $p^{ks} + d_i$ if $X_{p^{ks}+d} = X_0$ because the same generator is obtained when $h_{X_n} = m + 1$. Otherwise, the same process repeats for different seeds, not more than v times. □

Remark 3.2. More precise information on $d_i, i = 1, ..., v$ and v can be known by discussing a and p^k based on the Definition 2.1, Theorem 2.2, Lemma 2.1 and Remark 2.1.

4 Conclusion

This paper gives an improvement of most known and used random number generators based on modular reduction by introducing a new variable called the extension of the generator. The discussion on the importance of the topic and existing results is concise yet covers all the notions of importance. Sources that had great impact over time are referred to, as well as to some new high-quality manuscripts that represent an important connection of well researched notions with the ones that are to be discovered and improved. Afterwards, some important, well known facts and statements are mentioned since some results of this paper being their consequence. Finally, the results concerning the characteristics of the generators obtained by using the extension as well as the period length increase caused by extension, are given and briefly discussed.

Future work on Extended LCG will consist of investigation of randomness and period length properties, simulation and testing studies and similar empirical evidence issues, cryptography application possibilities and quality of encryption, as well as discussion on cracking this generator and comparative studies.

References

[1] A. Avdović, V. Jevremović, *Discrete Parameter-Free Zone Distribution and Its Application in Normality Testing*, Axioms, Vol. 12, 12 (2023). https://doi.org/10.3390/axioms12121087

[2] A. Avdović, V. Jevremović, *Quantile-Zone Based Approach to Normality Testing*, Mathematics, Vol. 10, 11 (2022). https://doi.org/10.3390/math10111828

[3] L. Devroye, *Non-Uniform Random Variate Generation*, Springer, New York, 1986.

[4] J. EICHENAUER, H. GROTHE, J. LEHN, A. TOPUZOĞLU, *A multiple recursive nonlinear congruential pseudo random number generator*, Manuscripta Mathematica, 59 (1987), 331–346. https://doi.org/10.1007/BF01174798

[5] G. S. FISHMAN, L. R. MOORE, *An exhaustive analysis of multiplicative congruential random number generators with modulus* $2^{31}-1$, SIAM Journal of Scientific and Statistical Computing, 7, (1986), 24-45. https://doi.org/10.1137/0907002

[6] G. S. FISHMAN, *Multiplicative Congruential Random Number Generators with Modulus* 2^{β} *: An Exhaustive Analysis for* $\beta = 32$ *and Partial Analysis for* $\beta = 48$, Mathematics of Computation, 54:189, (1990), 331-344. https://doi.org/10.1090/S0025-5718-1990-0993929-9

[7] A. T. FULLER, *The Period of Pseudo-Random Numbers Generated by Lehmer's Congruential Method*, The Computer Journal, 19:2, (1976), 173–177. https://doi.org/10.1093/comjnl/19.2.173

[8] J. GENTLE, *Random Number Genetarion and Monte Carlo Methods*, George Mason University, Fairfax, 2002.

[9] F. GOUALARD, *Drawing random floating-point numbers from an interval*, ACM Transactions on Modeling and Computer Simulation, 32 (3), (2022). https://hal.science/hal-03282794v4

[10] M. M. JACAK, P. JÓŹWIAK, J. NIEMCZUK, J.E. JACAK, *Quantum generators of random numbers*, Scientific Reports, 11:16108 (2021). https://doi.org/10.1038/s41598-021-95388-7

[11] V. JEVREMOVIĆ, A. AVDOVIĆ, *Control Charts Based on Quantiles - New Approaches*, Scientific Publications of the State University of Novi Pazar, Series A, Applied Mathematics, Informatics and Mechanics, Vol. 12, 2 (2020), 99-104. https://doi.org/10.5937/SPSUNP2002099J

[12] V. JEVREMOVIĆ, A. AVDOVIĆ, *Empirical Distribution Function as a Tool in Quality Control*, Scientific Publications of the State University of Novi Pazar, Series A, Applied Mathematics, Informatics and Mechanics, Vol. 12, 1 (2020), 37-46. https://doi.org/10.5937/SPSUNP2001037J

[13] D. E. KNUTH, *The Art of Computer Programming. Vol. 2, Seminumerical Algorythms - Third Eddition*, Addison-Wesley, Reading, Massachusetts, 1998.

[14] D. H. LEHMER, *Mathematical methods in large-scale computing unit*, in: Proceedings of a Second Symposium on Large-Scale Digital Calculating Machinery, Harvard University Press, Cambridge, Massachusetts, 1951, pp. 141–146.

[15] G. MARSAGLIA, *Random Number Generators*, Journal of Modern Applied Statistical Methods, 2:1 (2003), 2–13. 10.22237/jmasm/1051747320

[16] V. MULDER, A. MERMOUD, V. LENDERS, B. TELLENBACH, editors, *Trends in Data Protection and Encryption Technologies*, Springer Nature Switzerland, Cham, Springer Science+Business Media New York, 2023.

[17] S. K. PARK, K. W. MILLER, J. LEHN, *Random number generators: Good ones are hard to find*, Communications of the ACM, 31:10 (1988), 1192–1201. https://doi.org/10.1145/63039.63042

[18] M. SPIES, *Independent topical structures identification: Theoretical approach and proof-of-concept study*, Scientific Publications of the State University of Novi Pazar, Series A, Applied Mathematics, Informatics and Mechanics, Vol. 15, 1 (2023), 1-19. http://www.dunp.np.ac.rs/wp-content/uploads/2022/publikacije/serija-a/contents/vol.15no1-2023/SP-SUNP-15-1-23-1.pdf (accessed on 13 December 2023)

[19] H. C. TANG, *Modulus of Linear Congruential Random Number Generator*, Quality and Quantity, 39 (2005), 413-422. https://doi.org/10.1007/s11135-004-6788-6

[20] P. C. WU, *Multiplicative, Congruential Random-Number Generators with Multiplier* $\pm 2^{k_1} \pm 2^{k_2}$ *and Modulus* $2^p - 1$, ACM Transactions on Mathematical Software, 23:2 (1997), 255–265. https://doi.org/10.1145/264029.264056