Monte Carlo - Project

Dawid Kubkowski

December 22, 2024

Contents

1 Introduction

This report investigates the properties of several pseudorandom number generators (PRNGs), focusing on their periods and the results of statistical tests that evaluate their uniformity. The generators analyzed are:

- Linear Congruential Generator (LCG).
- Generalized Linear Congruential Generator (GLCG).
- RC4 stream cipher with specified parameters.
- Mersenne Twister (MT19937).

Additionaly, we will analyze the binary expansions of $\sqrt{2}$, e, and π, and perform the Frequency Monobit Test and the Frequency Test within a Block on these expansions.

2 Generators

2.1 LCG, GLCG, RC4

These PRNGs are described in the project description, file: *2024_monte_carlo_project1*.

2.2 Mersenne Twister Generator

The Mersenne Twister is a widely used pseudorandom number generator (PRNG) that was developed by Makoto Matsumoto and Takuji Nishimura in 1997. It is known for its high performance, large period, and relatively simple implementation. The name 'Mersenne Twister' comes from the fact that the generator's period length is a Mersenne prime, specifically $2^{19937} - 1$. This results in a very long period, making it suitable for applications requiring large sequences of random numbers, such as simulations, cryptography, and statistical modeling.

For a w-bit word length (typically $w = 32$), the Mersenne Twister generates integers in the range $[0, 2^w - 1]$. The Mersenne Twister is also known for passing many statistical tests for randomness and is used in various programming languages and software libraries, including NumPy, Python, and MATLAB.

For more detailed information on the Mersenne Twister algorithm, including its history and applications, please refer to the following link: `https://en.wikipedia.org/wiki/Mersenne_Twister`.

3 Tests

We would like to assess the quality of the generators, and we will do it by performing different statistical tests.

A statistical test is designed to evaluate a specific null hypothesis (H_0). In this context, the null hypothesis states that the sequence under consideration is random. In contrast, the alternative hypothesis (H_A) asserts that the sequence is not random.
In other words we test hypothesis:

$$H_0 : \text{The sequence is random}$$
$$H_A : \text{The sequence is not random.}$$

3.1 Chi-Square and Kolmogorov-Smirnov tests

Described in the project description, file: *2024_monte_carlo_project1*.

3.2 Frequency Test within a Block

The test comes from NIST Test Suite. Assuming that we have a random sequence of bits $(B_1, \ldots, B_n)$, we divide this sample into M-bit blocks and the idea is that the frequency of ones in the block should be around $M/2$, as would be expected under assumption of randomness.

The test evaluates the uniformity of the distribution of ones and zeros, the procedure is as follows:

1. Divide the binary sequence $(B_1, \ldots, B_n)$ into $N = \lfloor n/M \rfloor$ non-overlapping M-bit blocks. Discard any remaining bits that do not fit into a full block.

2. For each block, compute the proportion of ones using the formula:

$$\pi_i = \frac{1}{M} \sum_{j=1}^{M} B_{(i-1)M+j}, \quad i = 1, \ldots, N.$$

3. Compute the χ^2 statistic using the formula:

$$\chi^2 = 4M \sum_{i=1}^{N} \left(\pi_i - \frac{1}{2} \right)^2 .$$

4. Calculate the p-value using the incomplete gamma function:

$$p = \text{igamc}\left(\frac{N}{2}, \frac{\chi^2}{2}\right).$$

5. Compare the p-value to the significance level α:

   - If $p \geq \alpha$, do not reject the null hypothesis H_0 (the sequence is random).
   - If $p < \alpha$, reject the null hypothesis H_0 (the sequence is not random).

4 Methodology

In this section, we describe the methodology for conducting simulations of pseudorandom number sequences. It consists of three main steps:

1. **Generating the sample:** A sequence $(u_1, \ldots, u_n)$ of pseudorandom numbers of size $n = 10^6$ is generated using one of four specified random number generators: LCG, GLCG, RC4, MT19937.

2. **Statistical tests:** After generating the sequence of numbers, we perform a series of statistical tests to evaluate whether the sequence is uniform. In this step, we perform the following tests:

   - **Chi-Square Test:** This test checks whether the number of values in each bin (bucket) matches the expected count assuming a uniform distribution.

     (a) **10 buckets**

     $$[0, 0.1, 0.2, \ldots, 1]$$

     (b) M **buckets**, depending on the generator. Every generator considered in this project, by default, yields numbers from $\bar{M} = \{0, 1, \ldots, M-1\}$. These numbers are then scaled by M to produce $u_i \in [0, 1)$. Choosing M buckets ensures that we can test falling into each category, testing on discrete uniform distribution $U\{0, M-1\}$.

   - **Kolmogorov-Smirnov:** A second statistical test that evaluates another aspect of the generated distribution.

   - **Frequency Test within a Block:** A third test that examine the proportion of ones in each block.

3. **Second Level Testing:** For second level testing, we divide the generated sample ($n = 10^6$) into 100 subsets. For each subset, we perform a statistical test to obtain a set of p-values. If the null hypothesis (H_0) is true, the p-values should follow a uniform distribution. To check this, we perform the Chi-Square test on the set of p-values. A uniform distribution of p-values suggests that the null hypothesis holds, and the generator produces a uniform sequence.

4. **Significance Level:** All statistical tests in this analysis are conducted at the significance level $\alpha = 0.05$. This means that if the p-value of a test is less than 0.05, we reject the null hypothesis (H_0).

5 Results

5.1 LCG with parameters $M = 13$, $a = 1$, $c = 5$

Test	Statistic	p-value
Chi-square A	124259.645	0.000
Chi-square B	0.000	1.000
Kolmogorov-Smirnov	0.077	0.000
Block Frequency Test	5917.004	0.000

(a) Statistical tests for the LCG.

p-value	Decision
0.000	Reject
0.000	Reject
0.000	Reject
0.000	Reject

(b) Second level testing results.

Table 1: Statistical tests and second level testing for the LCG generator.

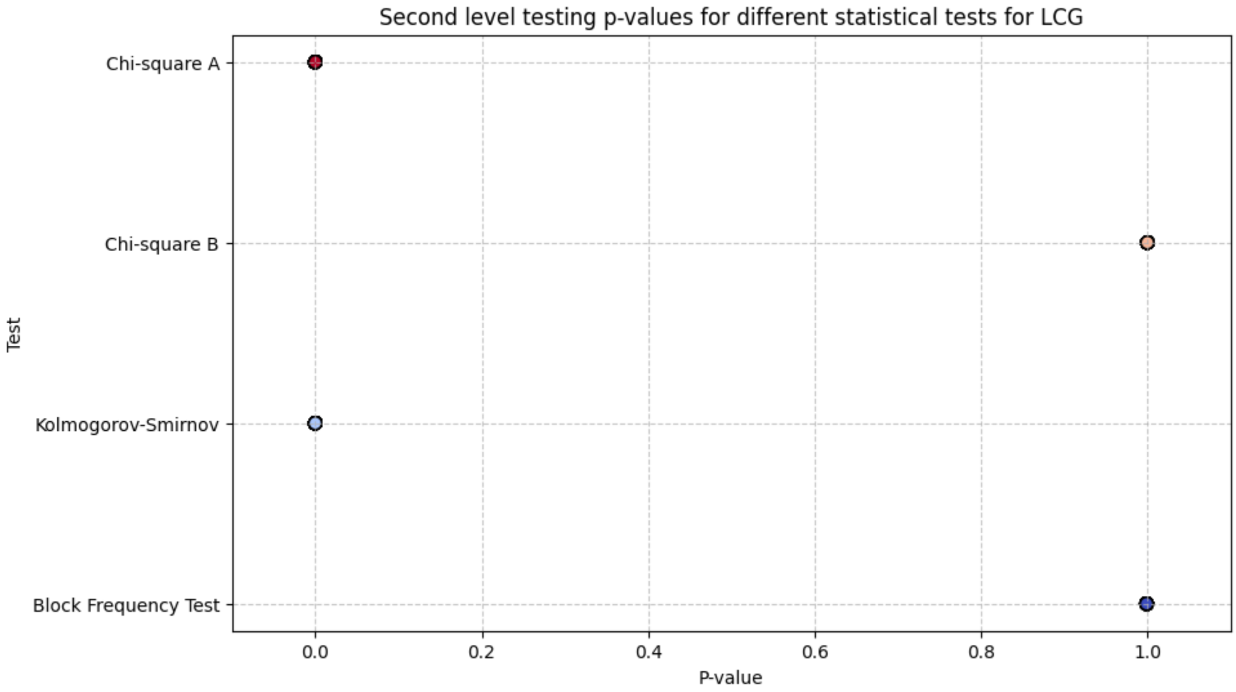

Figure 1: Second level p-values distribution for LCG generator.

The period of this generator was found to be 13 that does not depend on a seed, which means that in our sample, there are only 13 unique values, given by the set $\{\frac{i}{13} : i = 0, 1, \ldots, 12\}$.

For the Chi-square A test, let us consider the first sub-interval $[0, 0.1)$. Two observations fall into this category: $0 = \frac{0}{13}$ and $0.077 = \frac{1}{13}$. In our sample, we expect approximately $\frac{2 \cdot 10^6}{13} = 153846$ observations to fall into this sub-interval, while in a uniform distribution, we would expect $0.1 \cdot 10^6 = 10^5$ observations in $[0, 0.1)$. The difference between the observed and expected counts causes the test statistic to increase, as calculated by $(153846 - 100000)^2 = 53846^2$. There are also different bins that behave similarly.

Going next with a Chi-square B we always get p-values that equal to 1, second level testing rejects the randomness of the sample.

It appears that BFT (Block Frequency Test) is not rejecting the H_0 working with the smaller subset of the data, but the second level testing rejects the hypothesis.

5.2 GLCG$(2^{10}, \{3, 7, 68\})$

Test	Statistic	p-value
Chi-square A	908.442	0.000
Chi-square B	2555559.168	0.000
Kolmogorov-Smirnov	0.005	0.000
Block Frequency Test	0.154	1.000

(a) Statistical tests for the GLCG.

p-value	Decision
0.000	Reject
0.000	Reject
0.000	Reject
0.000	Reject

(b) Second level testing results.

Table 2: Statistical tests and second level testing for the GLCG generator.

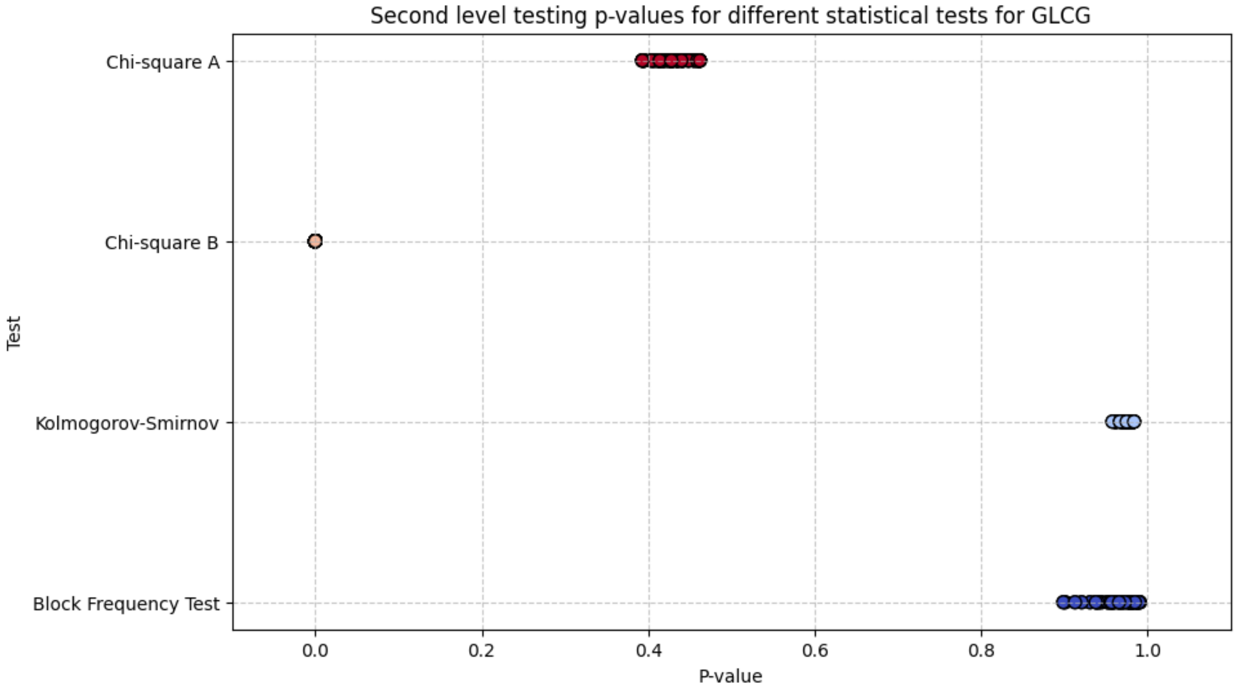

Figure 2: Second level p-values distribution for GLCG generator.

The BFT is the only test that does not reject the null hypothesis. However, after second-level testing, the null hypothesis can be rejected. When considering the entire sample, the tests provide clear and decisive outcomes. Nevertheless, in the second-level testing, we observe non-uniformly distributed p-values, indicating that the generator fails to produce truly random numbers.

5.3 RC4 with $m = 32,\ L = 10,\ K = 1000$

Key K of length L changes after 1000 generated observations.

Test	Statistic	p-value
Chi-square A	15519.794	0.000
Chi-square B	24.914	0.772
Kolmogorov-Smirnov	0.032	0.000
Block Frequency Test	3988.636	0.000

(a) Statistical tests for the RC4.

p-value	Decision
0.000	Reject
0.192	Cannot Reject
0.000	Reject
0.000	Reject

(b) Second level testing results.

Table 3: Statistical tests and second level testing for RC4 generator.

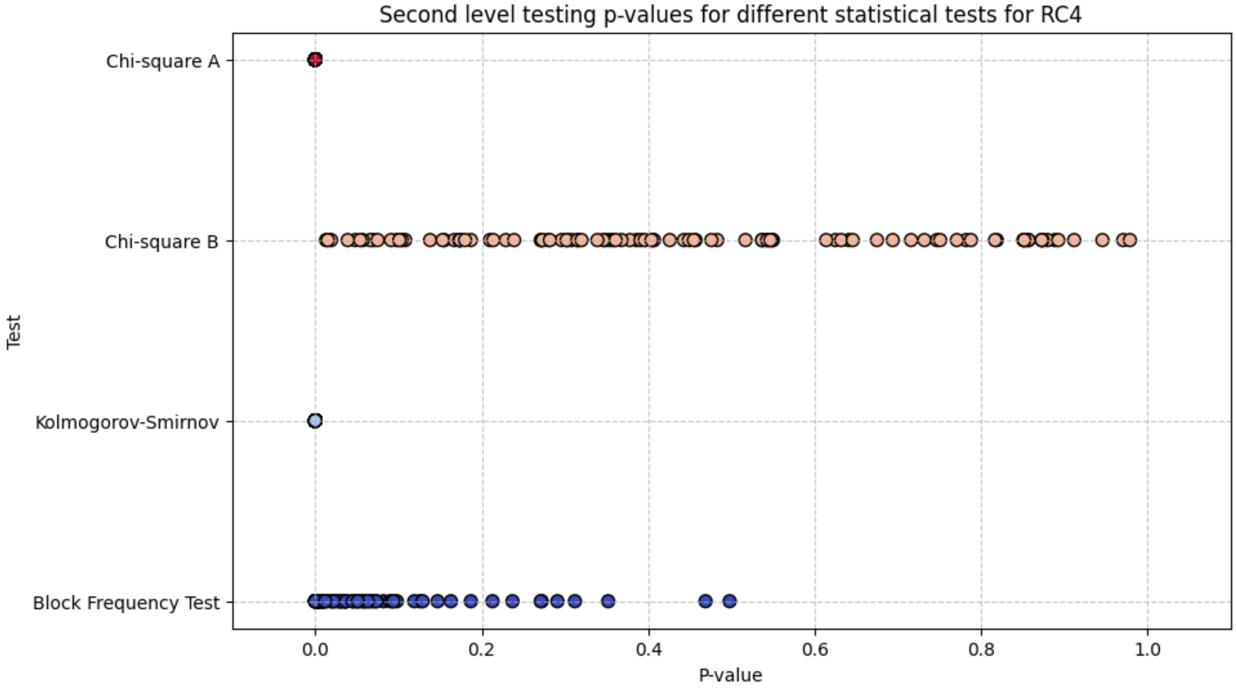

Figure 3: Second level p-values distribution for RC4 generator.

The RC4(32) stream cipher generator produces random numbers that follow a discrete uniform distribution $U\{0, 31\}$, as evidenced by the Chi-square B test, which fails to reject the null hypothesis. Furthermore, the generator successfully passes second-level testing.

5.4 MT

Test	Statistic	p-value
Chi-square A	9.941	0.355
Kolmogorov-Smirnov	0.001	0.234
Block Frequency Test	123.000	0.059

(a) Statistical tests for the MT.

p-value	Decision
0.554	Cannot Reject
0.237	Cannot Reject
0.384	Cannot Reject

(b) Second level testing results.

Table 4: Statistical tests and second level testing for the MT.

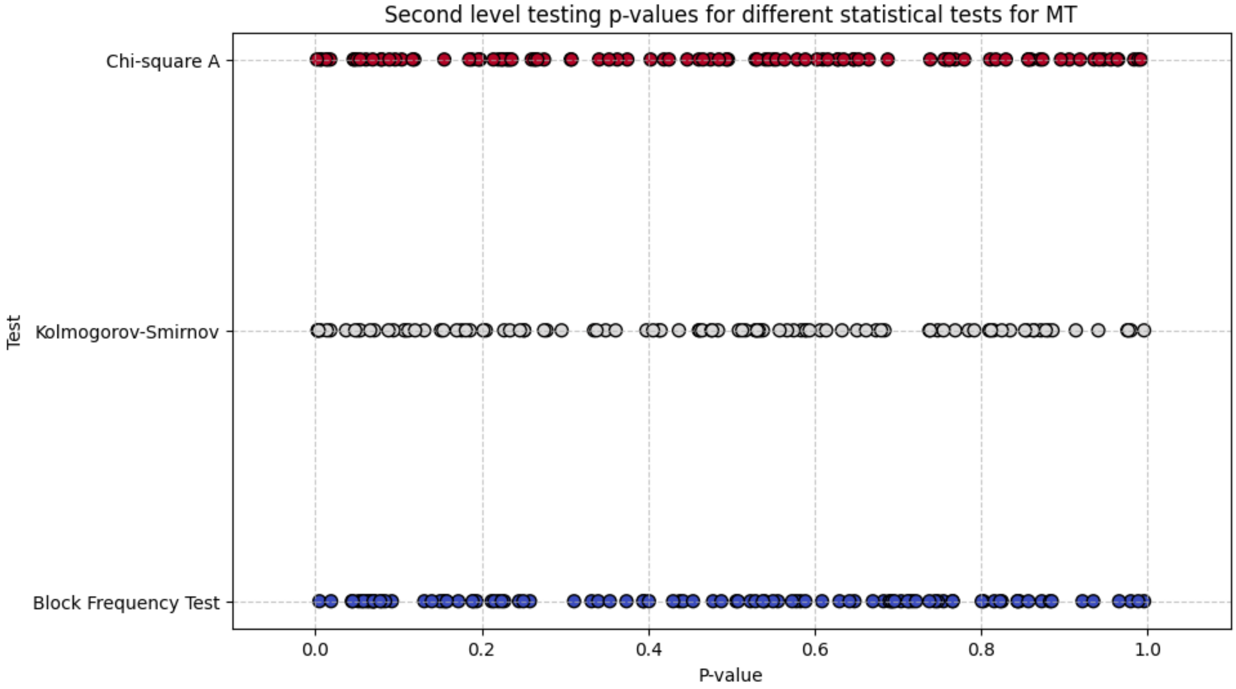

Figure 4: Second level p-values distribution for MT generator.

The Mersenne Twister (MT) PRNG passes all: Chi-square test, the Kolmogorov-Smirnov test, and the Block Frequency Test. Additionally, it successfully passes second-level testing. This makes it a robust and reliable random number generator, widely regarded as an excellent choice for pseudo-random number generation (PRNG) due to its high-quality output and performance.

The Chi-square B test was not conducted because the sample size of $n = 10^6$ is too small relative to the range of possible values, 2^{32}, making the test unsuitable for assessing a uniform distribution over $U\{0, 2^{32}\}$.

6 Binary expansions

In this study, we performed a series of statistical tests to evaluate the randomness of the binary expansions of π, e, and $\sqrt{2}$, treated as binary sequences. The analysis involved two primary tests:

1. Frequency Monobit Test (FMT).
2. Block Frequency Test (BFT).

The expansions can be found at:

- π: `http://www.math.uni.wroc.pl/~rolski/Zajecia/data.pi`
- e: `http://www.math.uni.wroc.pl/~rolski/Zajecia/data.e`
- $\sqrt{2}$: `http://www.math.uni.wroc.pl/~rolski/Zajecia/data.sqrt2`

Number	BFT p-value	FMT p-value
π	0.533	0.614
e	0.829	0.927
$\sqrt{2}$	0.106	0.818

(a) Statistical tests for the sample data.

BFT p-value	FMT p-value
0.637	0.554
0.367	0.851
0.319	0.679

(b) Second level testing results.

Table 5: Statistical tests and second level testing for the sample data.

Results

The results of both the FM Test and BFT, as well as the second-level testing, did not reject the null hypothesis of randomness for the binary sequences derived from the decimal expansions of π, e, and $\sqrt{2}$. This indicates that these expansions exhibit characteristics consistent with random binary sequences.

Figure	**Function**
Figure 1, Table 1	`run_test_for_generator("LCG", seed=1)`
Figure 2, Table 2	`run_test_for_generator("GLCG", seed=[1, 1, 1])`
Figure 3, Table 3	`run_test_for_generator("RC4", seed=1)`
Figure 4, Table 4	`run_test_for_generator("MT", seed=1)`
Table 5	`perform_tests(datasets, subset_count=100)`

Table 6: Functions and Corresponding Figures