1 Introduction

The main objective of the current work is to understand the concept and implementation of a **Random generator** (Congruential Random number generator (RNG) as in this case) in accomplishing the following tasks :

1. To develop a Congruential RNG, whose validity is tested with various parameters namely, (c, p and seed x_o). Subsequently, the reliability of this random generator is verified through the **a)** square test (two-dimensional),**b)** cube test [2, 4] (three-dimensional) and by **c)** changing other paramaters like c,p and seed.

2. To generate a homogenous distribution of random points inside a circle, by choosing appropriate values of radii and angular coordinates.

3. Further, testing the developed random generator with the χ^2 test [3].

2 Algorithmic Description

The current section succintly explains the algorithm behind Congruential RNG. This algorithm requires the user to input three positive integers : c, p and seed (x_o). Successive random numbers can be generated by the following relation:

$$x_i = (cx_{i-1})\mathbf{mod}p \tag{1}$$

Implictly, this means that random numbers generated are not entirely random! Rather, they do follow a definite recurrence relation, which repeats itself after large iterations (if p is chosen to be large). This is possible by choosing a large maximal period (p-1) which . The condition for the maximal period can be obtained if p is a Merseinne number [2, 5] [1]

3 Results

3.1 Task 1

In this task, the first part is accomplished by considering values of c, p and seed x_o mentioned in the Figure captions respectively. Subsequently, the performance of the RNG is verified by a two-dimensional plot (square test), cube test and also by changing other parameters : seed, c and p. Figures **??** illustrate this.

3.2 Task 2

The distribution of random numbers, can be observed to be homogeneous as shown in Figure 6. Two figures with small and large values of p are plotted to demonstrate that the homegenity is clearly visible in the latter.

[1] Note that the codes in the current work do not test the Merseinne condition. It is assumed that the user enters the value of p, which follows the Merseinne condition as available in [1]

3.3 Task 3

For the χ^2 test in this subsection, eight bins have been chosen, giving a probability of 0.125 to locate a random number. Different random number generators are obtained on choosing different values of seed (x_o), c and p [2].
Three sequence of random numbers have been generated, which have been tabulated in Table 1.

Table 1: χ^2 value computed with different sequence of random numbers

Seed	**c**	**p**	χ^2	**Percentage points**
5	3	61	4.36364	25-50 %
4	10	107	4.8889	25-50 %
3	25	127	7.63636	50-75 %

4 Discussion

4.1 Task 1

As seen from Figures **??** (square test), the random numbers seem to lie along the lines/planes in a specific pattern. Simialr condition is verified in the three-dimensional cubic plot also. Further, the above observations hold true for different random generators also, thus verifying the reliability of our method.

4.2 Task 2

The mathematical derivation behind the generaton of uniformly distributed random numbers as seen in **??** is outlined in this subsection. Let us use polar coordinates in the circle, characterized by r and θ, signifying the radius of an infinitesimal element from the center and angle of rotation from the horinzontal axis respectively. The outer radius of the entire circle is denoted by R (taken to be unity, in this work).
Consider an infinitesimal portion of the colored region in the circle, which is at a distance of r, with an interior angle of $d\theta$ and length dr.

$$Area\ of\ the\ infinitesimal\ region\, dA = rdrd\theta \tag{2}$$

Let the angle $d\theta$ of this infinitesimal portion of be rotated till 2π, so that it can be transformed into an infinitesimal rectangular portion , along cartesian coordinate system (signifying, uniform distribution). Let z denote the random variable distributed in this rectangular uniform distrubution system. Since, the areas of integration (circle and rectangle) must be the same, we can express this mathematically as :

$$z = \int P(z)\ dz = \int\ dz \tag{3}$$

$$Now, z = \int_0^r \int_0^{2\pi} P(A)\ rdrd\theta,\ where\ P(A)\ =\ \frac{1}{\pi R^2} \tag{4}$$

This can be simplified as

$$z = \frac{r^2}{R^2}\ =\ r^2, as\ R\ is\ unity. \tag{5}$$

Or simply,

$$r = \sqrt{z} \tag{6}$$

[2]Note : The program has a limit of numbers upto 200 (stored in an array). So, the maximal period has to be subsequently chosen to be less than 200.

For $z_i \in [0,1]$, the polar coordinates of uniformly distributed random numbers in the circle can be computed as:

$$r_i = \sqrt{rand[0,1]} \; and \; \theta_i = 2\pi rand[0,1] \tag{7}$$

4.3 Task 3

From the Results outline for Task 3 in Table 1, we can conclude that our random number generator is reliable (when compared with the percentage points in [3]).

References

[1] List of known mersenne prime numbers - primenet. `https://www.mersenne.org/primes/`. (Accessed on 10/02/2017).

[2] Hans Hermann. Lecture no tes on introduction to computationaly physics, 2017.

[3] Donald E. Knuth. *The Art of Computer Programming, Volume 2 (3rd Ed.): Seminumerical Algorithms*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1997.

[4] George Marsaglia. Random numbers fall mainly in the planes. *Proceedings of the National Academy of Sciences*, 61(1):25–28, 1968.

[5] Wikipedia. Mersenne prime — wikipedia, the free encyclopedia, 2017.

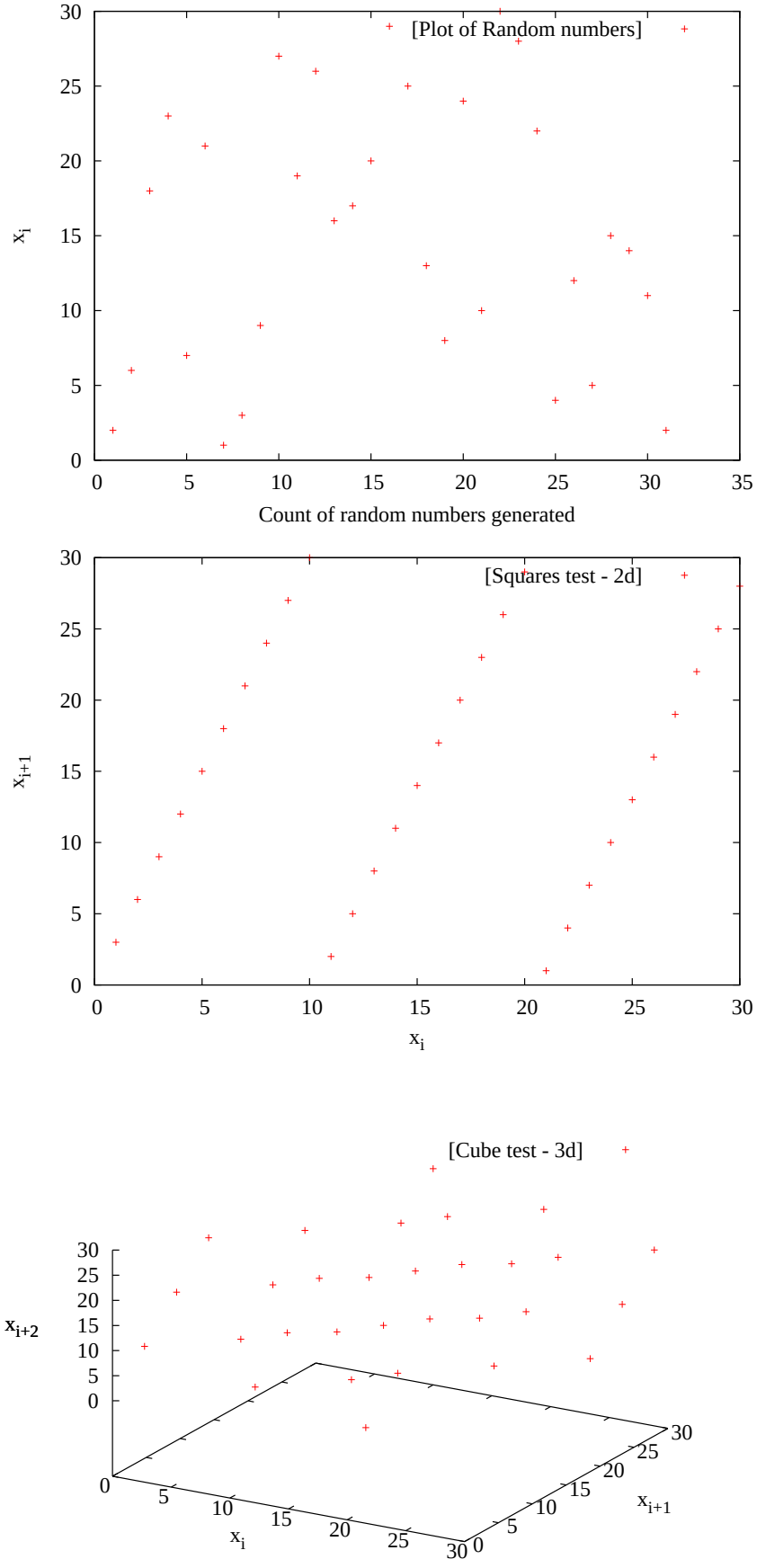

Figure 1: Squares and Cube test for c,p and seed taken to be 3, 31 and 2 respectively

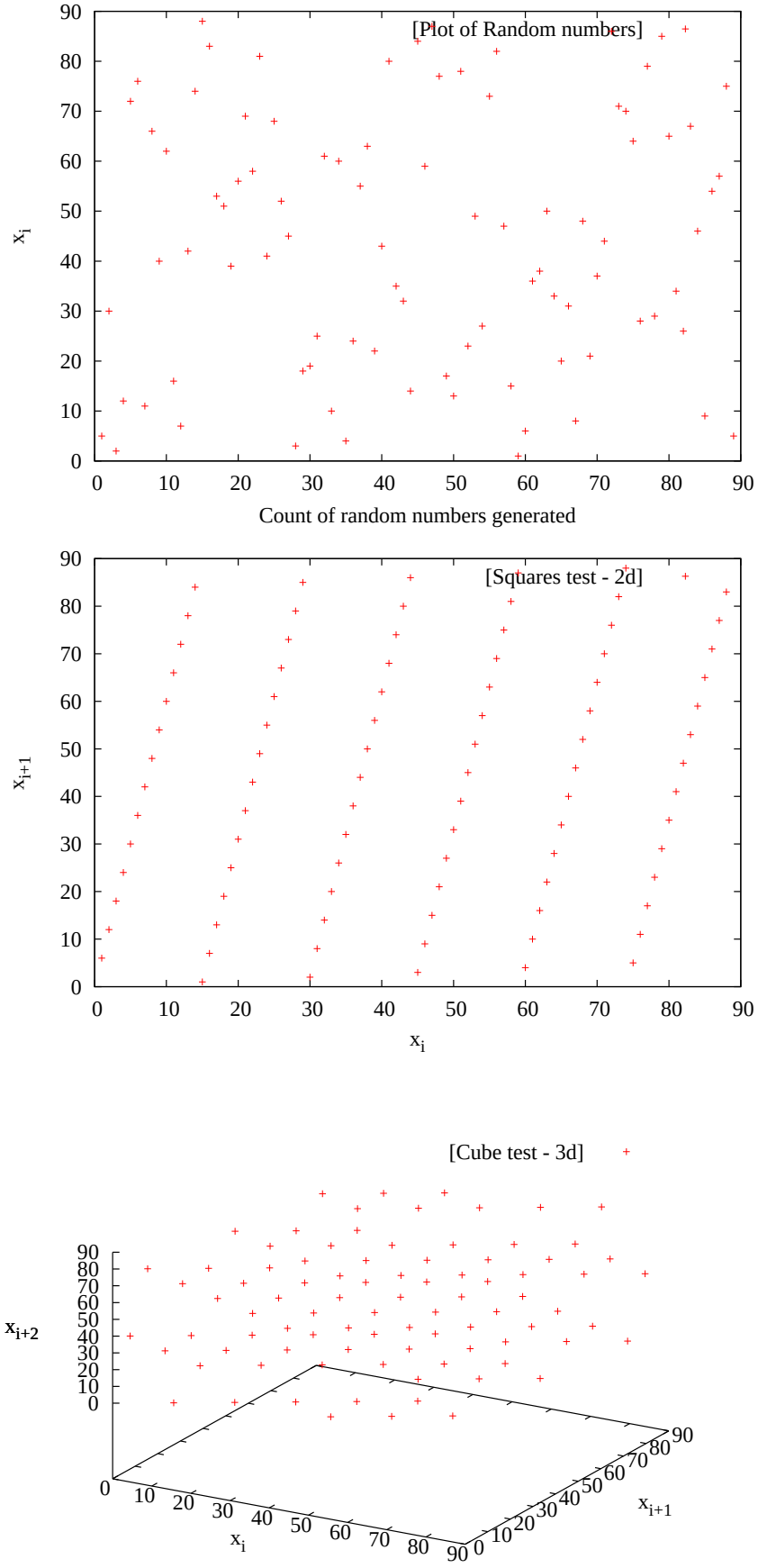

Figure 2: Squares and Cube test for c,p and seed taken to be 5, 6 and 89 respectively

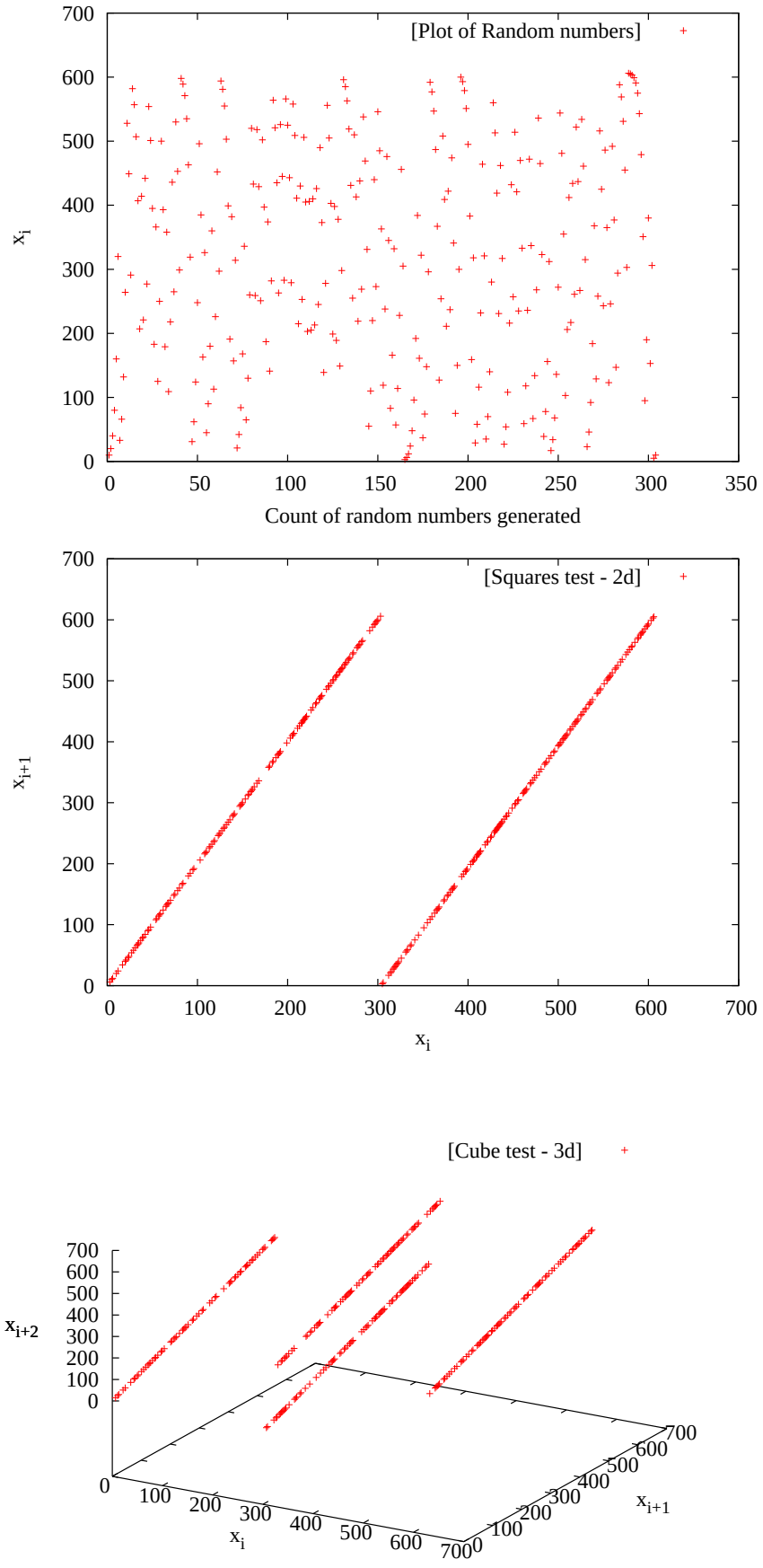

Figure 3: Squares and Cube test for c,p and seed taken to be 10, 2 and 607 respectively

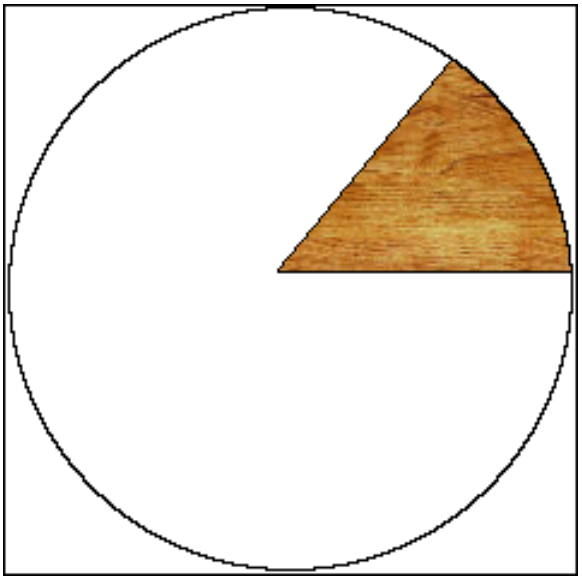

Figure 4: Circle, in which random numbers will be homogeneously distributed

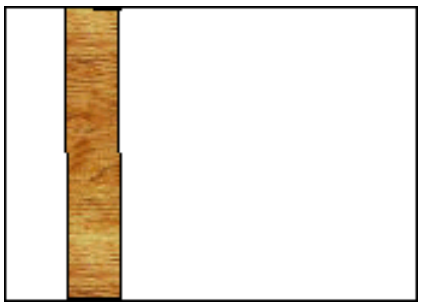

Figure 5: Rectangle, signifying uniform distribution - Obtained by transforming the circular portion with same area

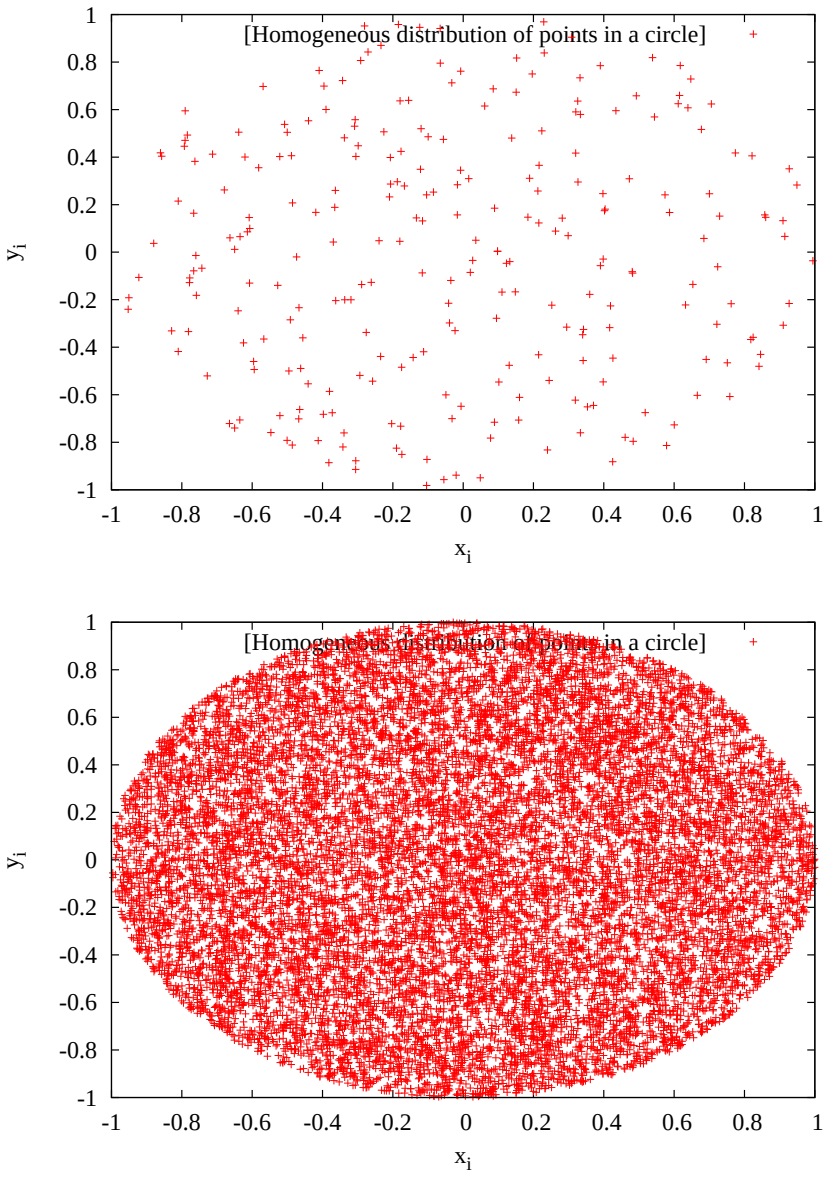

Figure 6: Uniformly generated random numbers with the parameters : $r_{seed} = 5$,$\theta_{seed} = 3$,respective c values of 8,9 and p taken to be 521 (above) and 216091 (below)