1 Introduction

Several small experiments on a basic congruential random number generator were conducted.

2 Algorithm Description

The congruential random number generator employed generates pseudo-random numbers x_i based on the linear recurrence relation $x_{i+1} = (c \cdot x_i) \bmod p$ where $c, p \in \mathbb{R}$.

3 Results

3.1 Task 1

3.1.1 Subtask 1.1

200 random numbers were generated using $c = 3$, $p = 31$ and plotted for the square test. As shown in figure 1, three lines were observed after normalizing the generated numbers with $x_i \leftarrow \frac{x_i}{p}$.

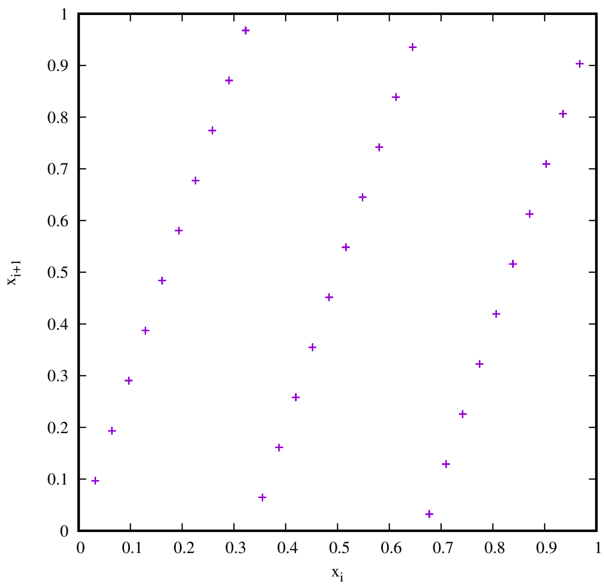

Figure 1: Square test for congruential random number generator with $c = 3$, $p = 31$.

3.1.2 Subtask 1.2

As in the previous task, 200 random numbers were generated using $c = 3$, $p = 31$ and plotted for the cube test. As shown in figure 2, regular patterns can be observed after normalizing the generated numbers with $x_i \leftarrow \frac{x_i}{p}$, but identifying planes is somewhat difficult owing to the spacing caused by the short period.

3.1.3 Subtask 1.3

The random number generator was modified to run with $c = 2836$, $p = 127773$ to yield a substantially longer period and improved pseudo-randomness. As evident in figures 3 and 4, regular patterns appear much less common.

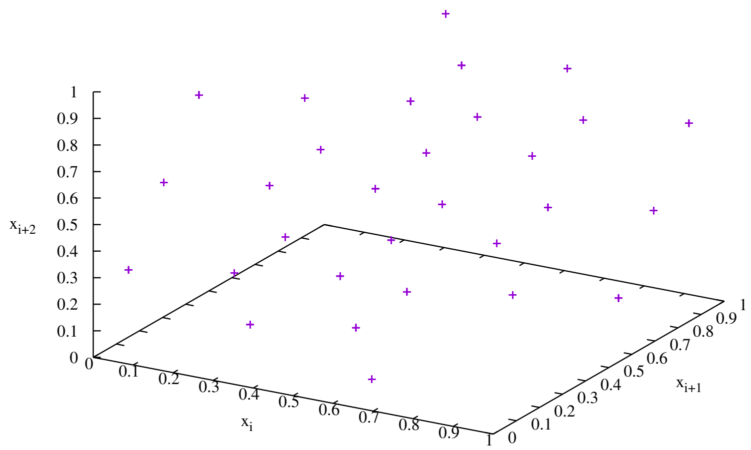

Figure 2: Cube test for congruential random number generator with $c = 3$, $p = 31$.

3.2 Task 2

In polar coordinates, the angle ϕ can be chosen from a uniform distribution as the setup is invariant to rotation about the centre of the circle. The radius coordinate r however needs to be transformed $r \leftarrow \sqrt{z}$, $z \sim \text{Unif}(0, 1)$ as sampling from a uniform distribution would yield too much mass near the centre of the circle. Plotting 200 random numbers generated with $c = 2836$, $p = 127773$ on a circle with radius $R = 1$ and center $(0, 0)$ yields the result shown in figure 5.

3.3 Task 3

The code as submitted with this report was run several times to generate 2000 random numbers distributed over $k = 10$ bins.
For $c = 3$, $p = 31$, the average score was $\chi^2 = 0.038$ which seems extremely unlikely when comparing to Knuth's table [1].
For $c = 2836$, $p = 127773$, the average score was $\chi^2 = 6.778$ which is around the $p = 40\%$ mark on Knuth's table [1].
Clearly and as expected, $c = 3$, $p = 31$ make for a poor result in terms of randomness, whereas $c = 2836$, $p = 127773$ already achieve quite a respectable score.

4 Discussion

The results were in line with the theoretical expectations from class. I personally had issues getting decent plots as I had shied away from Gnuplot until now. Also, my c++ is somewhat rusty and I apologise for my somewhat ugly code.

References

[1] Knuth, Ervin D., *The art of computer programming*, Addison Wesley, Massachusetts, 3rd edition, 1997.

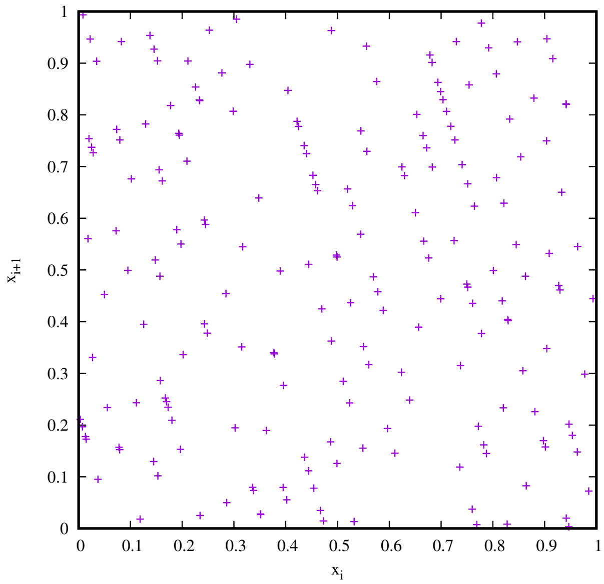

Figure 3: Square test for congruential random number generator with $c = 2836$, $p = 127773$.

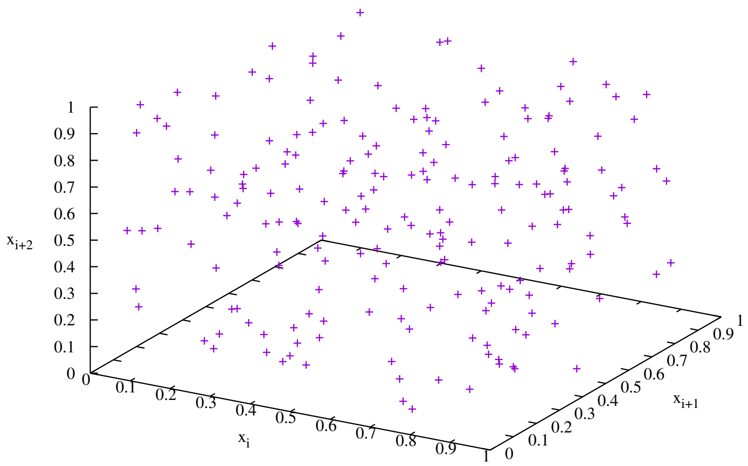

Figure 4: Cube test for congruential random number generator with $c = 2836$, $p = 127773$.

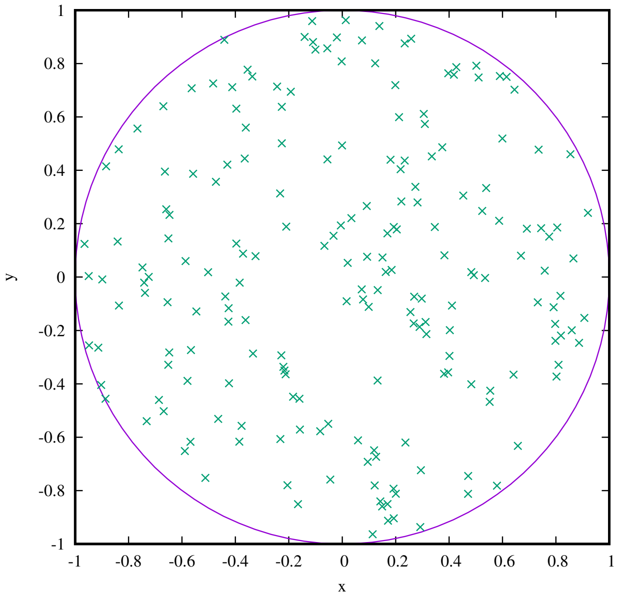

Figure 5: Output of congruential random number generator with $c = 2836$, $p = 127773$ plotted on circle with radius $R = 1$ and center $(0, 0)$.