1 Introduction

- congruential random number generator
- transformation method
- χ^2 test of random number generator

2 Algorithm Description

2.1 congruential random number generator

The algorithm of congruential random number generator is

$$x_0 \neq 0$$
$$x_i = cx_{i-1} \bmod p$$

where c,p,x_0 are positive integers and p is prime number. The square test is created by plotting the points (x_{i-1}, x_i) in the $x - y$ plane.

2.2 transformation method

The transformation method is

$$z = \int_0^z P(z')dz' = \int_0^y P(y')dy'$$

where $P(z) = 1 \text{ if } z \in [0,1] \, 0 \text{ otherwise}$. For example, to generate a homogeneous distribution of random points inside a circle using polar coordinates ϕ and r, two uniformly distributed random number ϕ' and r' map to ϕ and r by

$$r = R\sqrt{r'}$$
$$\phi = 2\pi\phi'$$

The relation is obtained by assuming the density of points are the same in the regions $[0, 2\pi] \times [0, R]$ and $\{(x, y)|x^2 + y^2 \leq R^2\}$. Without the loss of generality, pick the density $\rho = 1$,

$$\frac{1}{2\pi R}\int_0^{r'} \mathrm{d}r \int_0^{\phi'} \mathrm{d}\phi = \frac{1}{\pi R^2}\int_0^{r} r\mathrm{d}r \int_0^{\phi} \mathrm{d}\phi$$
$$r'\phi' = \frac{1}{R}r^2\phi$$

If we shrink the range of r' and ϕ' in $[0, 1]$, it becomes

$$Rr'2\pi\phi' = \frac{1}{R}r^2\phi$$

Therefore, the map is obtained by let $\phi = 2\pi\phi'$ and $r = R\sqrt{r'}$.

2.3 χ^2 test

Generate n random numbers and count the appearance of random number N_i in k intervals with equal width. Since the range of random number is $p - 1$ for congruential random number generator, the interval width is $l = \frac{p-1}{k}$. Then, χ^2 is calculated by

$$\chi^2 = \sum_{i=1}^{k} \frac{(N_i - np_i)^2}{np_i}$$

where $p_i = \frac{1}{k}$ is the probability of a random number in the ith interval.

3 Results

3.1 Task 1

The square test of congruential random number generator with $c = 3$, $p = 101$, $x_0 = 1$ is plotted in Fig.(1) below. The random number x is in the range $[0, 1]$ by dividing the period p. $p - 1$ random numbers are generated in this case. Besides, the square test of rand() function in the standard C

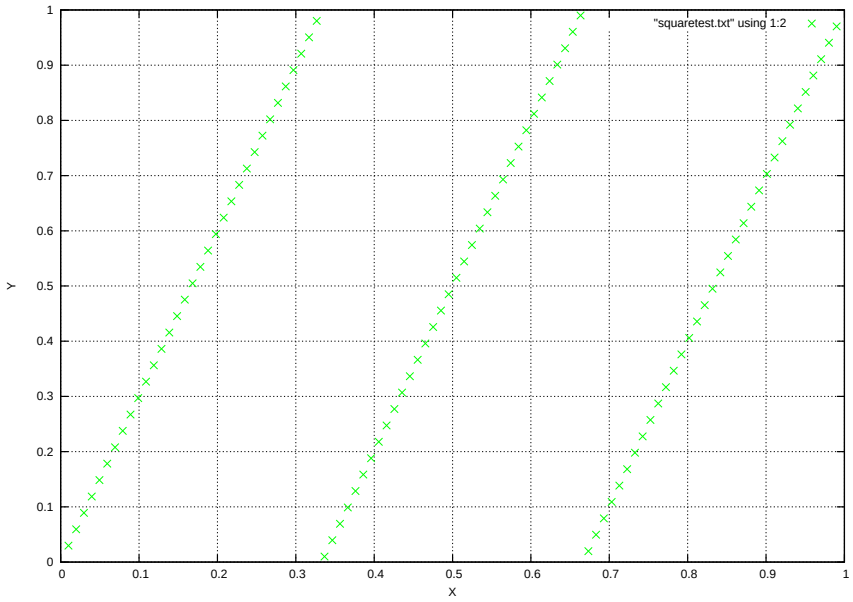


Figure 1: Square test of congruential random number generator($c = 3$, $p = 101$, $x_0 = 1$)

library(stdlib.h) is plot in Fig.(2) The congruential random number generator has a linear relation of

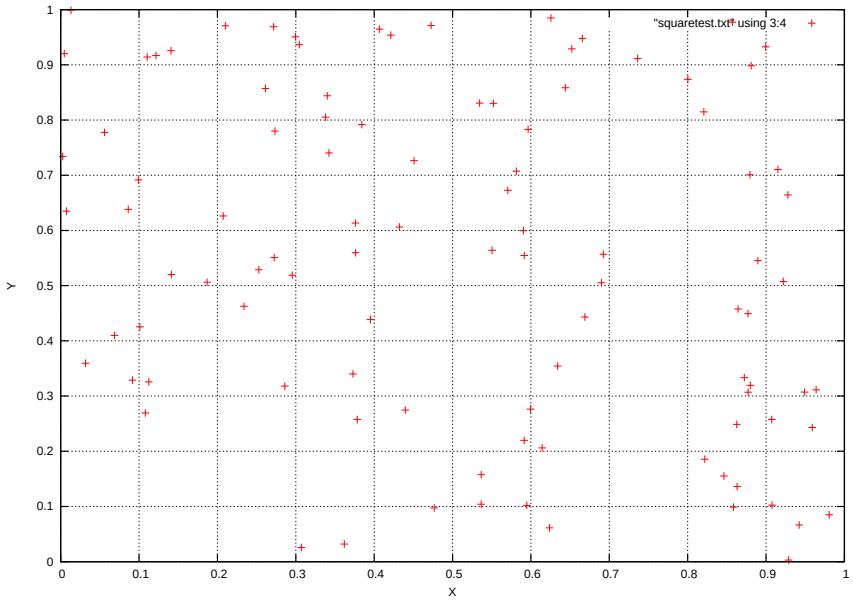


Figure 2: Square test of rand() function in stdlib.h

$x_{i-1} - x_i$ but the rand() doesn't have such property.

3.2 Task 2

The homogeneous distribution of random points inside a circle is plot in Fig.(3).

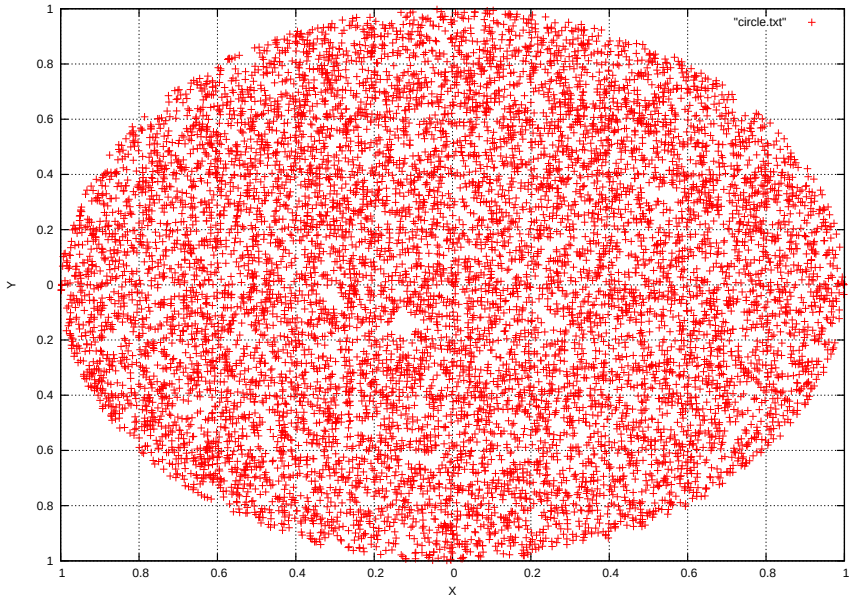


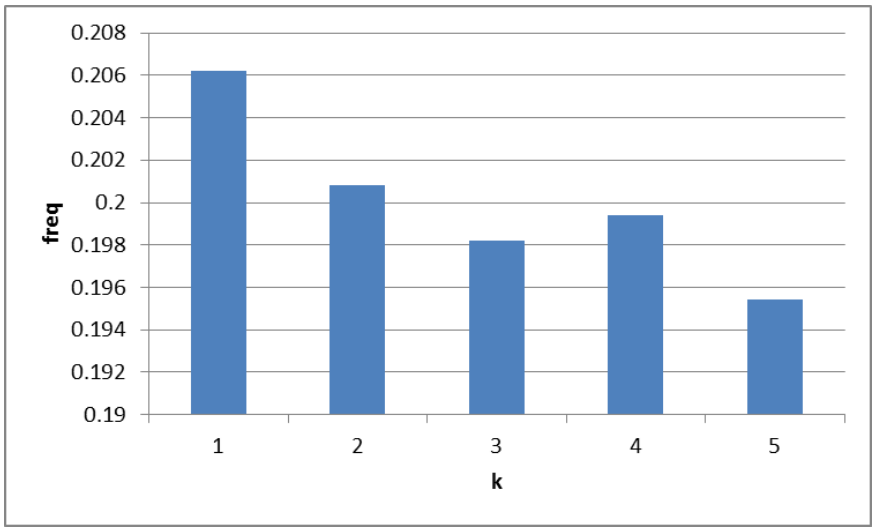
Figure 3: Homogeneous distribution of random points inside a circle($R = 1$)

3.3 Task 3

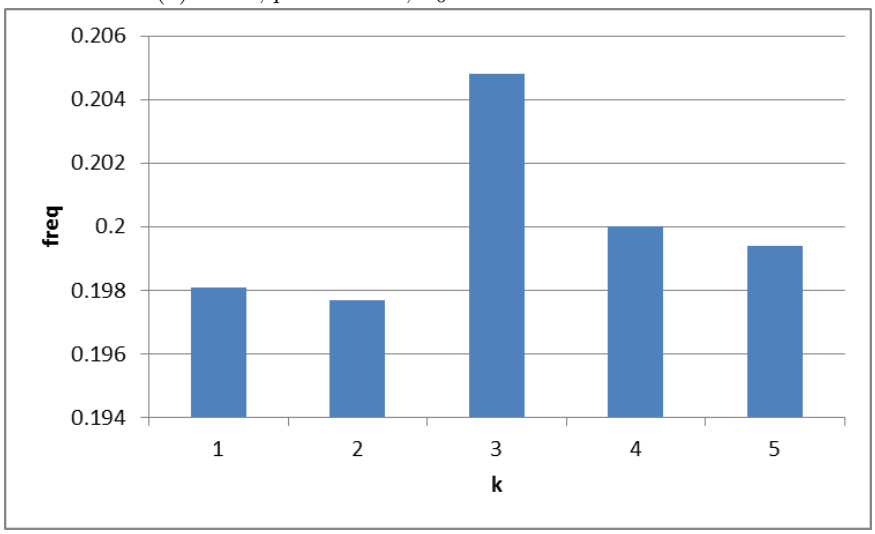
The χ^2 test of congruential random number generator($c = 7$, $p = 2^{19} - 1$, $x_0 = 1$) is plot in Fig.(4a) where $n =$ 1e4 and $k = 5$. $\chi^2 = 3.192$ and $P = 0.5$ according to the χ^2 table in [1]. By changing $c = 3$, $p = 2^{17} - 1$, the χ^2 test is plot in Fig.(4b). $\chi^2 = 1.615$ and $P = 0.25$.

References

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



(a) $c = 7$, $p = 2^{19} - 1$, $x_0 = 1$



(b) $c = 3$, $p = 2^{17} - 1$, $x_0 = 1$

Figure 4: χ^2 test of congruential random number generator