Program-M9

Devansh Shukla
I18PH021

a) Calculate 10 pseudorandom numbers for RNG(263, 71, 100, 79) and RNG(13, 0, 31, 1).

b) Write & execute a Fortran program to solve the above problem. Compare your numerical and programmed results. Plot Random Applet with your generated random numbers

1 Theory

Lehmer invented the *multiplicative congruential algorithm*, which is now-a-days used in many random number generators. It is a type of linear congruential generator(LCG).

It involves three initial integer parameters a, c, m and an initial value x_0 called the seed.

$$x_{k+1} = (ax_k + c) \bmod m \tag{1}$$

For example, $a = 13$, $c = 0$, $m = 31$ and $x_0 = 1$ gives the following sequence,

$$1,\ 13,\ 14,\ 27,\ 10,\ 6,\ 16,\ 22,\ 7,\ 29,\ 5,\ 3... \tag{2}$$

The numbers in Eq.(2) looks random but actually they are pseudorandom numbers tied together by Eq.(1)

2 Numerical Solution

$$\text{Using,} \quad I_{n+1} = (AI_n + C) \bmod M \tag{3}$$

i) For $RNG(263,\ 71,\ 100,\ 79)$

$$A = 263;\ \ C = 71;\ \ M = 100;\ \ I_0 = 79;$$

$$\begin{aligned}
I_1 &= (AI_0 + C) \bmod M \\
&= (263 \times 79 + 71) \bmod 100 \\
&= 20848 \bmod 100 \\
&= 48 \\
I_2 &= (AI_1 + C) \bmod M \\
&= (263 \times 48 + 71) \bmod 100 \\
&= 12695 \bmod 100 \\
&= 95 \\
I_3 &= (AI_2 + C) \bmod M \\
&= (263 \times 95 + 71) \bmod 100 \\
&= 25056 \bmod 100 \\
&= 56 \\
I_4 &= (AI_3 + C) \bmod M \\
&= (263 \times 56 + 71) \bmod 100 \\
&= 14799 \bmod 100 \\
&= 99 \\
I_5 &= (AI_4 + C) \bmod M \\
&= (263 \times 99 + 71) \bmod 100 \\
&= 26108 \bmod 100 \\
&= 8 \\
I_6 &= (AI_5 + C) \bmod M \\
&= (263 \times 8 + 71) \bmod 100 \\
&= 2175 \bmod 100 \\
&= 75 \\
I_7 &= (AI_6 + C) \bmod M \\
&= (263 \times 75 + 71) \bmod 100 \\
&= 19796 \bmod 100 \\
&= 96
\end{aligned} \tag{4}$$

$$
\begin{aligned}
I_8 &= (AI_7 + C) \bmod M \\
&= (263 \times 96 + 71) \bmod 100 \\
&= 25319 \bmod 100 \\
&= 19 \\
I_9 &= (AI_8 + C) \bmod M \\
&= (263 \times 19 + 71) \bmod 100 \\
&= 5068 \bmod 100 \\
&= 68 \\
I_{10} &= (AI_9 + C) \bmod M \\
&= (263 \times 68 + 71) \bmod 100 \\
&= 17955 \bmod 100 \\
&= 55
\end{aligned} \tag{5}
$$

$$
I = [79,\ 48,\ 95,\ 56,\ 99,\ 8,\ 75,\ 96,\ 19,\ 68,\ 55] \tag{6}
$$

ii) For $RNG(13,\ 0,\ 31,\ 1)$

$$
\begin{aligned}
I_1 &= (AI_0 + C) \bmod M \\
&= (13 \times 1 + 0) \bmod 31 \\
&= 13 \bmod 31 \\
&= 13 \\
I_2 &= (AI_1 + C) \bmod M \\
&= (13 \times 13 + 0) \bmod 31 \\
&= 169 \bmod 31 \\
&= 14 \\
I_3 &= (AI_2 + C) \bmod M \\
&= (13 \times 14 + 0) \bmod 31 \\
&= 182 \bmod 31 \\
&= 27 \\
I_4 &= (AI_3 + C) \bmod M \\
&= (13 \times 27 + 0) \bmod 31 \\
&= 351 \bmod 31 \\
&= 10 \\
I_5 &= (AI_4 + C) \bmod M \\
&= (13 \times 10 + 0) \bmod 31 \\
&= 130 \bmod 31 \\
&= 6 \\
I_6 &= (AI_5 + C) \bmod M \\
&= (13 \times 6 + 0) \bmod 31 \\
&= 78 \bmod 31 \\
&= 16 \\
I_7 &= (AI_6 + C) \bmod M \\
&= (13 \times 16 + 0) \bmod 31 \\
&= 208 \bmod 31 \\
&= 22 \\
I_8 &= (AI_7 + C) \bmod M \\
&= (13 \times 22 + 0) \bmod 31 \\
&= 286 \bmod 31 \\
&= 7 \\
I_9 &= (AI_8 + C) \bmod M \\
&= (13 \times 7 + 0) \bmod 31 \\
&= 91 \bmod 31 \\
&= 29 \\
I_{10} &= (AI_9 + C) \bmod M \\
&= (13 \times 29 + 0) \bmod 31 \\
&= 377 \bmod 31 \\
&= 5
\end{aligned} \tag{7}
$$

$$I = [1,\ 13,\ 14,\ 27,\ 10,\ 6,\ 16,\ 22,\ 7,\ 29,\ 5] \tag{8}$$

3 Program Algorithm

NOTE: Blue-colored text represents variables in the algorithm, eg. variable.

1. Program open
2. Define A, C, M, R, x_0, x_1, i, and fmt
3. Open a file "random_no.dat" with write access.
4. Get input from user for A, C, M and x_0.
5. Get input from user for no. of random numbers n.
6. Open a do loop for index i from 0 to n.
7. Compute the value of x_1 according to given formula.
8. Write i, x_1, x_0 to file.
9. Set x_0 = x_1
10. End-do loop
11. Close file.
12. Program close

4 Program

4.1 Fortran program:

For computing the parameters

```
!=========================================
! rng.f90
! Author: Devansh Shukla
!-----------------------------------------
program rng_generator
    implicit none
    ! Define the variables
    integer :: A=0, C=0, M=0, x_0=0, x_1=0, i=0, n=10
    character(len=*), parameter :: fmt="(xI2,I6,I6)"
    ! Open data file
    open(unit=8, file="random_no.dat")
    ! Get input from user
    print *, "Enter A, C, M, x0"
    read *, A, C, M, x_0
    print *, "Enter no of random numbers(n)"
    read *, n
    print *, "-----------------"

    print "(xA2x, A6, xxA6)", "i", "I(i)", "I(i+1)"
    ! Compute
    do i = 0, n, 1
        ! Compute the pseudorandom number according to the
        ! given formula
        x_1 = mod(A*x_0 + C, M)
        write (*, fmt) i, x_0, x_1
        ! Writing the computed parameters to the data file
        write (8, fmt) i, x_0, x_1
        x_0 = x_1
    end do
    print *, "-----------------"
    ! Close file
    close(8)

end program rng_generator
```

4.2 Python program: Plots

```
#!/usr/bin/env python
"""
Author: Devansh Shukla
"""
import pandas as pd
import numpy as np
import matplotlib as mpl
```

```
import matplotlib.pyplot as plt
import matplotlib.gridspec as gridspec

plt.style.use("rcStyleSheet.mplstyle")
mpl.use("pgf")
plt.ioff()

df = pd.read_csv("random_no_1.dat", engine="python", delimiter=" ", header=None, skipinitialspace=True, comment="#")

fig = plt.figure(figsize=(4,4))
gs = gridspec.GridSpec(1, 1)
ax = fig.add_subplot(gs[0, 0])
ax.plot(df[1], df[2], "x", markersize=4, color="C0")
ax.set_xlim(0, 102)
ax.set_ylim(0, 102)
ax.set_xlabel(r"$x_{i}$")
ax.set_ylabel(r"$x_{i+1}$")
plt.suptitle("RNG(263,71,100,79)")
plt.title(r"$n=10$")
fig.savefig("outputs/rng_1.pdf")

df = pd.read_csv("random_no_2.dat", engine="python", delimiter=" ", header=None, skipinitialspace=True, comment="#")

fig = plt.figure(figsize=(4,4))
gs = gridspec.GridSpec(1, 1)
ax = fig.add_subplot(gs[0, 0])
ax.plot(df[1], df[2], "x", markersize=4, color="C0")
ax.set_xlim(0, 31)
ax.set_ylim(0, 31)
ax.set_xlabel(r"$x_{i}$")
ax.set_ylabel(r"$x_{i+1}$")
plt.suptitle("RNG(13,0,31,1)")
plt.title(r"$n=10$")
fig.savefig("outputs/rng_2.pdf")
```

5 Results

5.1 Terminal output

5.1.1 i)

```
 Enter A, C, M, x0
263 71 100 79
 Enter no of random numbers(n)
10
 -----------------
  i   I(i)  I(i+1)
  0    79    48
  1    48    95
  2    95    56
  3    56    99
  4    99     8
  5     8    75
  6    75    96
  7    96    19
  8    19    68
  9    68    55
 10    55    36
 -----------------
```

5.1.2 ii)

```
 Enter A, C, M, x0
13 0 31 1
 Enter no of random numbers(n)
10
 -----------------
  i   I(i)  I(i+1)
  0     1    13
  1    13    14
  2    14    27
  3    27    10
  4    10     6
  5     6    16
  6    16    22
  7    22     7
  8     7    29
  9    29     5
 10     5     3
 -----------------
```

5.2 Data files

The data files have three columns: index i, x_i and x_{i+1}.

5.2.1 i)

```
 0    79    48
 1    48    95
 2    95    56
 3    56    99
 4    99     8
 5     8    75
 6    75    96
 7    96    19
 8    19    68
 9    68    55
10    55    36
```

5.2.2 ii)

```
 0     1    13
 1    13    14
 2    14    27
 3    27    10
 4    10     6
 5     6    16
 6    16    22
 7    22     7
 8     7    29
 9    29     5
10     5     3
```

5.3 Plots

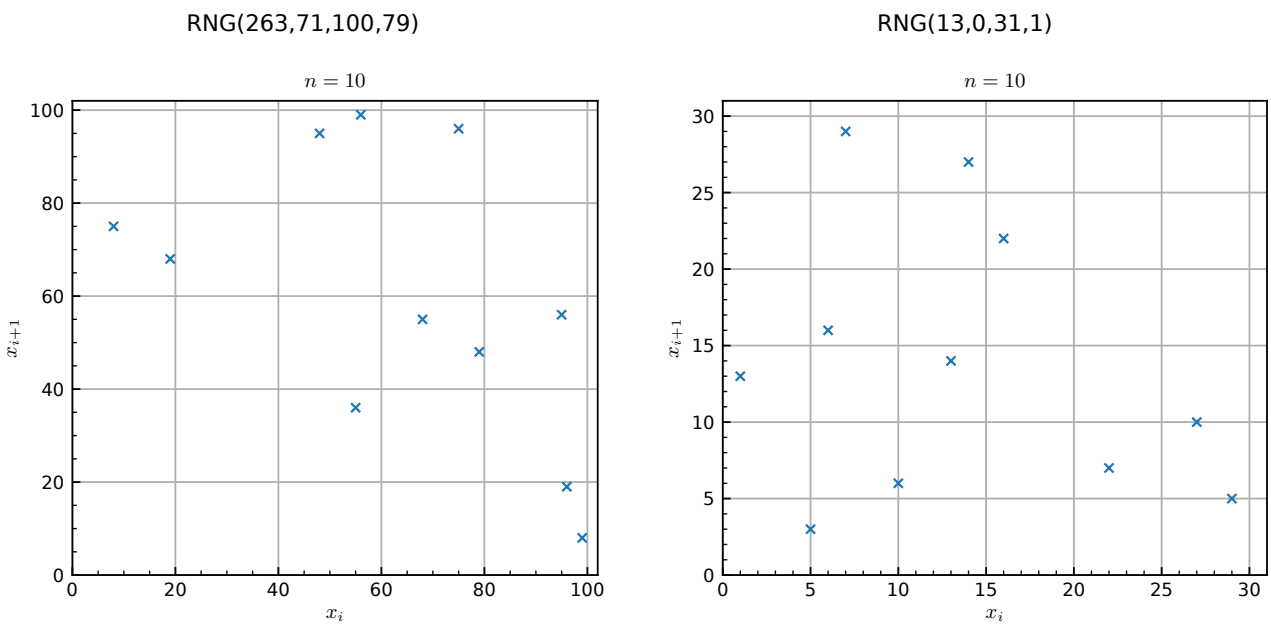

Figure 1: Random Applets

5.4 Random numbers generated:

$$\begin{aligned} \textbf{i)}: &\quad x = [79,\ 48,\ 95,\ 56,\ 99,\ 8,\ 75,\ 96,\ 19,\ 68,\ 55] \\ \textbf{ii)}: &\quad x = [1,\ 13,\ 14,\ 27,\ 10,\ 6,\ 16,\ 22,\ 7,\ 29,\ 5] \end{aligned} \tag{9}$$

6 Remarks

The programs can be used to compute pseudorandom numbers according to the defined parameters and seed.

The random numbers computed numerically and via the program are in agreement.