

Київський національний університет імені Тараса Шевченка  
Факультет комп'ютерних наук та кібернетики  
Кафедра системного аналізу та теорії прийняття рішень

Звіт  
з лабораторної роботи № 1  
**«Генерування псевдовипадкових чисел»**

Виконав  
студент групи К-23

Флакей Р.Р.

Київ - 2022

---

## Постановка задачі

---

Написати програму, що реалізує десять генераторів псевдовипадкових чисел. Кожний генератор викликати за допомогою меню, яке реагує на ввід цілого числа: 1, ... , 10. Згенерувати послідовність псевдовипадкових чисел, яка має якнайдовший період (не менше 100).

Побудувати гістограму, яка ілюструє розподіл чисел на інтервалах  $[0;1]$  (для нормального розподілу),  $[-3;3]$  (для нормального розподілу),  $[0; 100]$  – для решти розподілів. Гістограму подати у вигляді таблиці. Наприклад, для рівномірного розподілу вона виглядатиме приблизно так. Частота обчислюється як дріб, чисельником якого є кількість потраплянь випадкових чисел в певний інтервал, в знаменником – повна кількість згенерованих чисел.

Інтервал Частота

$[0; 0,1]$	0.05
$[0.1;0.2]$	0.15
$[0.2;0.3]$	0.1
$[0.3;0.4]$	0.12
$[0.4;0.5]$	0.1
$[0.5;0.6]$	0.15
$[0.6;0.7]$	0.05
$[0.7;0.8]$	0.08
$[0.8;0.9]$	0.16
$[0.9;1.0]$	0.04

Генератори псевдовипадкових чисел, як правило, породжують ціле число  $X$ , яке лежить в інтервалі від 0 до деякого заздалегідь заданого числа  $m$ . Тому дійсні псевдовипадкові числа, рівномірно розподілені між 0 і 1, обчислюються за формулою  $U = X/m$ .

# I. МЕТОДИ ГЕНЕРУВАННЯ РІВНОМІРНО РОЗПОДІЛЕНИХ ЧИСЕЛ

## 1. Лінійний конгруентний метод. [Кнут, т.2., с. 29–39]

$$X_{n+1} = (aX_n + c) \bmod m,$$

$$U_{n+1} = \frac{X_{n+1}}{m}, n \geq 0,$$

де  $m$  – модуль,  $m > 0$ ,  $a$  – множник,  $0 \leq a < m$ ,  $c$  – приріст,  $0 \leq c < m$ ,  $X_0$  – початкове значення,  $0 \leq X_0 < m$ .

- 1) числа  $c$  і  $m$  є взаємно простими;
- 2) число  $b = a - 1$  є кратним числу  $p$  для кожного простого числа  $p$ , яке є дільником числа  $m$ ;
- 3) число  $b$  є кратним 4, якщо число  $m$  є кратним 4.

Обрані коефіцієнти:

- $X_0 = 42949672$
- $a = 82589933$
- $c = 4294967279$
- $m = 4294967291$

Результат:

```
C:\Windows\System32\cmd.exe - lab1.exe
8 : The method of relations
9 : Logarithm method for generating an indicative dist
10: Ahrens method for generating a gamma distribution
-1: --Quit--

-> 1
*How many elements -> 1000

Select a method:
  1) preset value
  2) own value
-> 1

  Range          Frequency
[0.0;0.1)        0.10
[0.1;0.2)        0.10
[0.2;0.3)        0.10
[0.3;0.4)        0.10
[0.4;0.5)        0.09
[0.5;0.6)        0.10
[0.6;0.7)        0.11
[0.7;0.8)        0.10
[0.8;0.9)        0.11
[0.9;1.0]        0.10
```

## 2. Квадратичний конгруентний метод [Кнут, т.2., с. 46, 57 (вправа 8)]

$$X_{n+1} = (dX_n^2 + aX_n + c) \bmod m,$$

$$U_{n+1} = \frac{X_{n+1}}{m}, n \geq 0.$$

**Вибір параметрів.** Цей вибір визначається наступною теоремою: квадратична конгруентна послідовність, визначена числами  $m, a, c, d$  і  $X_0$ , має період  $m$  тоді і лише тоді, коли виконуються чотири умови:

- 1) числа  $c$  і  $m$  є взаємно простими;
- 2) числа  $d$  і  $a-1$  є кратними числу  $p$  для всіх чисел  $p$ , які є простими непарними дільниками числа  $m$ ;
- 3) число  $d$  є парним і  $d \equiv a-1 \pmod{4}$ , якщо число  $m$  є кратним 4;  
число  $d \equiv a-1 \pmod{2}$ , якщо число  $m$  є кратним 2;
- 4)  $d \not\equiv 3c \pmod{9}$ , якщо число  $m$  є кратним 3.

### Обрані коефіцієнти:

- $X_0 = 42949672$
- $a = 4294967197$
- $d = 4294967231$
- $c = 4294967279$
- $m = 4294967291$

### Результат:

```
C:\Windows\System32\cmd.exe - lab1.exe

8 : The method of relations
9 : Logarithm method for generating an indic
10: Ahrens method for generating a gamma dis
-1: --Quit--

-> 2
*How many elements -> 1000

Select a method:
  1) preset value
  2) own value
-> 1

Range      Frequency
[0.0;0.1)  0.09
[0.1;0.2)  0.09
[0.2;0.3)  0.09
[0.3;0.4)  0.09
[0.4;0.5)  0.09
[0.5;0.6)  0.11
[0.6;0.7)  0.11
[0.7;0.8)  0.11
[0.8;0.9)  0.11
[0.9;1.0]  0.11
```

### 3. Числа Фібоначчі [Кнут, т.2., с. 47]

$$X_{n+1} = (X_n + X_{n-1}) \bmod m, n \geq 0.$$

$$U_{n+1} = \frac{X_{n+1}}{m}$$

Обрані коефіцієнти:

- $X0 = 1247437$
- $X1 = 224743647$
- $m = 4294967291$

Результат:

```
C:\Windows\System32\cmd.exe - lab1.exe
-1:  --Quit--
-> 3
*How many elements -> 1000
Select a method:
  1) preset value
  2) own value
-> 1

Range      Frequency
[0.0;0.1)  0.10
[0.1;0.2)  0.11
[0.2;0.3)  0.10
[0.3;0.4)  0.10
[0.4;0.5)  0.10
[0.5;0.6)  0.09
[0.6;0.7)  0.09
[0.7;0.8)  0.10
[0.8;0.9)  0.11
[0.9;1.0]  0.09
```

#### 4. Обернена конгруентна послідовність [Кнут, т.2., с. 53, 61 (вправа 36) ]

$$X_{n+1} = (aX_n^{-1} + c) \bmod p,$$

$$U_{n+1} = \frac{X_{n+1}}{m}, n \geq 0,$$

де  $p$  – просте число, число  $X_n$  набуває значень із множини  $\{0, 1, \dots, p-1, \infty\}$ , а обертання визначається за правилами  $0^{-1} = \infty$ ,  $\infty^{-1} = 0$ . В інших випадках  $XX^{-1} \equiv 1 \bmod p$ . [Кнут, т.2., с. 53]

Вибір параметрів. Обернена конгруентна послідовність

$$X_{n+1} = (aX_n^{-1} + c) \bmod 2^e, X_0 = 1, e \geq 3$$

має період  $2^{e-1}$ , якщо  $a \bmod 4 = 1$  і  $c \bmod 4 = 2$ .

#### Обрані коефіцієнти:

- $X_0 = 17$
- $a = 29$
- $c = 18$
- $m = 6543$

#### Результат:

```
C:\Windows\System32\cmd.exe - lab1.exe
-1:  --Quit--

-> 4
*How many elements -> 1000

Select a method:
  1) preset value
  2) own value
-> 1

Range      Frequency
[0.0;0.1)   0.10
[0.1;0.2)   0.11
[0.2;0.3)   0.09
[0.3;0.4)   0.11
[0.4;0.5)   0.09
[0.5;0.6)   0.11
[0.6;0.7)   0.10
[0.7;0.8)   0.10
[0.8;0.9)   0.10
[0.9;1.0]   0.10
```

## 5. Метод об'єднання [Кнут, т.2., с. 55]

$$Z_n = (X_n - Y_n) \bmod m,$$
$$0 \leq X_n < m, \quad 0 \leq Y_n < m' \leq m,$$
$$U_{n+1} = \frac{Z_{n+1}}{m}, \quad n \geq 0.$$

Обрані коефіцієнти:

- $m = 4294967291$
- $X - \text{method01}()$
- $Y - \text{method02}()$

Результат:

```
C:\Windows\System32\cmd.exe - lab1.exe

For numbers generator by method 1:
Select a method:
1) preset value
2) own value
-> 1

For numbers generator by method 2:
Select a method:
1) preset value
2) own value
-> 1

Range      Frequency
[0.0;0.1)  0.10
[0.1;0.2)  0.11
[0.2;0.3)  0.10
[0.3;0.4)  0.09
[0.4;0.5)  0.09
[0.5;0.6)  0.10
[0.6;0.7)  0.11
[0.7;0.8)  0.11
[0.8;0.9)  0.11
[0.9;1.0]  0.10
```

## II. МЕТОДИ ГЕНЕРУВАННЯ НОРМАЛЬНО РОЗПОДІЛЕНИХ ЧИСЕЛ

$$N(0,1): F(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{t^2}{2}} dt$$

### 6. Правило “3 сігма” [Мейн, Савитч, с. 119]

$$X_n = m + (sum - 6)\sigma,$$

де  $m$  – медіана,  $\sigma$  – дисперсія,  $sum$  – сума дванадцяти випадкових чисел, рівномірно розподілених на інтервалі  $[a, b]$ . Якщо  $[a, b] = [0; 1]$ , то  $m = 0$ , а  $\sigma = 1$ . Правило 3-сігма стверджує, на проміжку  $[m-3\sigma; m+3\sigma]$  міститься 99,7% всіх випадкових чисел, що мають розподіл  $N(m, \sigma^2)$ . Отже для побудови гістограми розподілу  $N(0,1)$  достатньо обмежитись інтервалом  $[-3; 3]$ .

### Обрані коефіцієнти:

- $X - method01()$
- $m = 4294967291$
- $\sigma = 1$

### Результат:

```
C:\Windows\System32\cmd.exe - lab1.exe

-> 6
*How many elements -> 1000

Select a method:
  1) preset value
  2) own value
-> 1

For numbers generator by method 1:
  Range          Frequency
[-3.0;-2.4)      0.00
[-2.4;-1.8)      0.02
[-1.8;-1.2)      0.07
[-1.2;-0.6)      0.16
[-0.6; 0.0)      0.20
[0.0 ; 0.6)      0.25
[0.6 ; 1.2)      0.17
[1.2 ; 1.8)      0.09
[1.8 ; 2.4)      0.03
[2.4 ; 3.0]      0.01
```



## 7. Метод полярних координат [Кнут, т.2., с. 146]

7.1. Нехай  $U_1$  і  $U_2$  – випадкові числа, взяті із генеральної сукупності всіх чисел, рівномірно розподілених на інтервалі  $[0; 1]$ . Виконати такі перетворення.

$$V_1 \leftarrow 2U_1 - 1,$$

$$V_2 \leftarrow 2U_2 - 1.$$

Числа  $V_1$  і  $V_2$  належать генеральній сукупності чисел, рівномірно розподілених на інтервалі  $[-1; 1]$ .

7.2.  $S \leftarrow V_1^2 + V_2^2$ .

7.3. Якщо  $S \geq 1$ , виконати пункти 7.1 і 7.2.

7.4. Виконати такі перетворення.

$$X_1 \leftarrow V_1 \sqrt{\frac{-2 \ln S}{S}},$$

$$X_2 \leftarrow V_2 \sqrt{\frac{-2 \ln S}{S}}.$$

7.5. Видати числа  $X_1$  і  $X_2$ .

Обрані коефіцієнти:

- $U - method01()$

Результат:

```
C:\Windows\System32\cmd.exe - lab1.exe

-> 7
*How many elements -> 1000

Select a method:
  1) preset value
  2) own value
-> 1

For numbers generator by method 1:
  Range          Frequency
[-3.0;-2.4)      0.01
[-2.4;-1.8)      0.03
[-1.8;-1.2)      0.13
[-1.2;-0.6)      0.23
[-0.6; 0.0)      0.35
[0.0 ; 0.6)      0.38
[0.6 ; 1.2)      0.26
[1.2 ; 1.8)      0.13
[1.8 ; 2.4)      0.04
[2.4 ; 3.0]      0.01
```

## 8. Метод співвідношень [Кнут, т.2., с. 155]

- 8.1. Згенерувати дві незалежні випадкові величини, рівномірно розподілені на інтервалі  $[0; 1]$ :  $U \neq 0$  і  $V$ .
- 8.2.  $X \leftarrow \sqrt{\frac{8}{e}} \frac{V - \frac{1}{2}}{U}$ .
- 8.3. (Необов'язкова перевірка верхньої грані.) Якщо  $X^2 \leq 5 - 4e^{\frac{1}{4}U}$ , то результатом є число  $X$ . Завершити алгоритм.
- 8.4. (Необов'язкова перевірка нижньої грані.) Якщо  $X^2 \geq \frac{4e^{-1.35}}{U} + 1.4$ , то повернутися на крок 8.1.
- 8.5. (Остаточна перевірка.) Якщо  $X^2 \leq -4 \ln U$ , то видати число  $X$  і завершити алгоритм, інакше повернутися на крок 8.1.

### Обрані коефіцієнти:

- $U - method01()$
- $V - method02()$

### Результат:

```
C:\Windows\System32\cmd.exe - lab1.exe
-> 8
*How many elements -> 1000

Select a method:
  1) preset value
  2) own value
-> 1

For numbers generator by method 1:
For numbers generator by method 2:
  Range      Frequency
[-3.0;-2.4)  0.01
[-2.4;-1.8)  0.02
[-1.8;-1.2)  0.05
[-1.2;-0.6)  0.11
[-0.6; 0.0)  0.14
[0.0 ; 0.6)  0.18
[0.6 ; 1.2)  0.14
[1.2 ; 1.8)  0.07
[1.8 ; 2.4)  0.02
[2.4 ; 3.0]  0.00
```

### III. Методи генерування інших розподілів

#### 9. Метод логарифму для генерування показового розподілу [Кнут, т.2., с. 157]

$$F(x) = 1 - e^{-\frac{x}{\mu}}, x \geq 0.$$

Якщо  $y = F(x) = 1 - e^{-\frac{x}{\mu}}$ , то  $x = F^{-1}(y) = -\mu \ln(1 - y)$ . Таким чином, величина

$$x = -\mu \ln(1 - U),$$

має експоненційний розподіл, якщо число  $U$  належить генеральній сукупності випадкових величин, рівномірно розподілених на інтервалі  $[0; 1]$ . Оскільки величина  $1 - U$  має той же самий розподіл, формулу можна спростити:

$$x = -\mu \ln U.$$

Обрані коефіцієнти:

- $U - method01()$
- $\mu - 20$

Результат:

```
C:\Windows\System32\cmd.exe - lab1.exe

-> 9
*How many elements -> 1000

Select a method:
  1) preset value
  2) own value
-> 1

For numbers generator by method 2:
  Range          Frequency
[ 0; 10)         0.35
[10; 20)         0.24
[20; 30)         0.16
[30; 40)         0.09
[40; 50)         0.07
[50; 60)         0.04
[60; 70)         0.02
[70; 80)         0.01
[80; 90)         0.00
[90;100]         0.01
```

## 10. Метод Аренса для генерування гамма-розподілу порядку $a > 1$

[Кнут, т.2., с. 159]

$$F(x) = \frac{1}{\Gamma(a)} \int_0^x t^{a-1} e^{-t} dt, x \geq 0, a > 0.$$

10.1. (Генерування кандидата.) Згенерувати випадкове число  $U$ , що належить генеральній сукупності випадкових величин, рівномірно розподілених на інтервалі  $[0; 1]$ . Виконати операції

$$Y \leftarrow \text{tg}(\pi U),$$

$$X \leftarrow \sqrt{2a-1}Y + a - 1.$$

10.2. (Перша перевірка.) Якщо  $X \leq 0$ , повернутися на крок 10.1.

10.3. (Остаточна перевірка.) Згенерувати випадкове число  $V$ , що належить генеральній сукупності випадкових величин, рівномірно розподілених на інтервалі  $[0; 1]$ .

Якщо  $V > (1 + Y^2) \exp\left((a-1) \ln\left(\frac{X}{a-1}\right) - \sqrt{2a-1}Y\right)$ , повернутися на крок 10.1.

10.4. Видати число  $X$ .

### Обрані коефіцієнти:

- $U - \text{method01}()$
- $V - \text{method02}()$
- $a - 17$

### Результат:

```
C:\Windows\System32\cmd.exe - lab1.exe
10: Ahrens method for generating a gamma d
-1: --Quit--

-> 10
*How many elements -> 1000

Select a method:
  1) preset value
  2) own value
-> 1

For numbers generator by method 1:
For numbers generator by method 2:
  Range      Frequency
[ 0; 10)      0.02
[10; 20)      0.42
[20; 30)      0.12
[30; 40)      0.00
[40; 50)      0.00
[50; 60)      0.00
[60; 70)      0.00
[70; 80)      0.00
[80; 90)      0.00
[90; 100]     0.00
```