

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ

ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(ДГТУ)

Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

Лабораторная работа №3

по дисциплине «Теория псевдослучайных генераторов»

Выполнила: обучающаяся гр. ВКБ41

Хороших Я. Д

Проверили:

Артамонова Е. А.

г. Ростов-на-Дону

2025 г.

**Лабораторная работа №3**

**«Генератор Фибоначчи псевдослучайных чисел на регистрах сдвига с линейной обратной связью»**



Рисунок 1 – Значения варианта

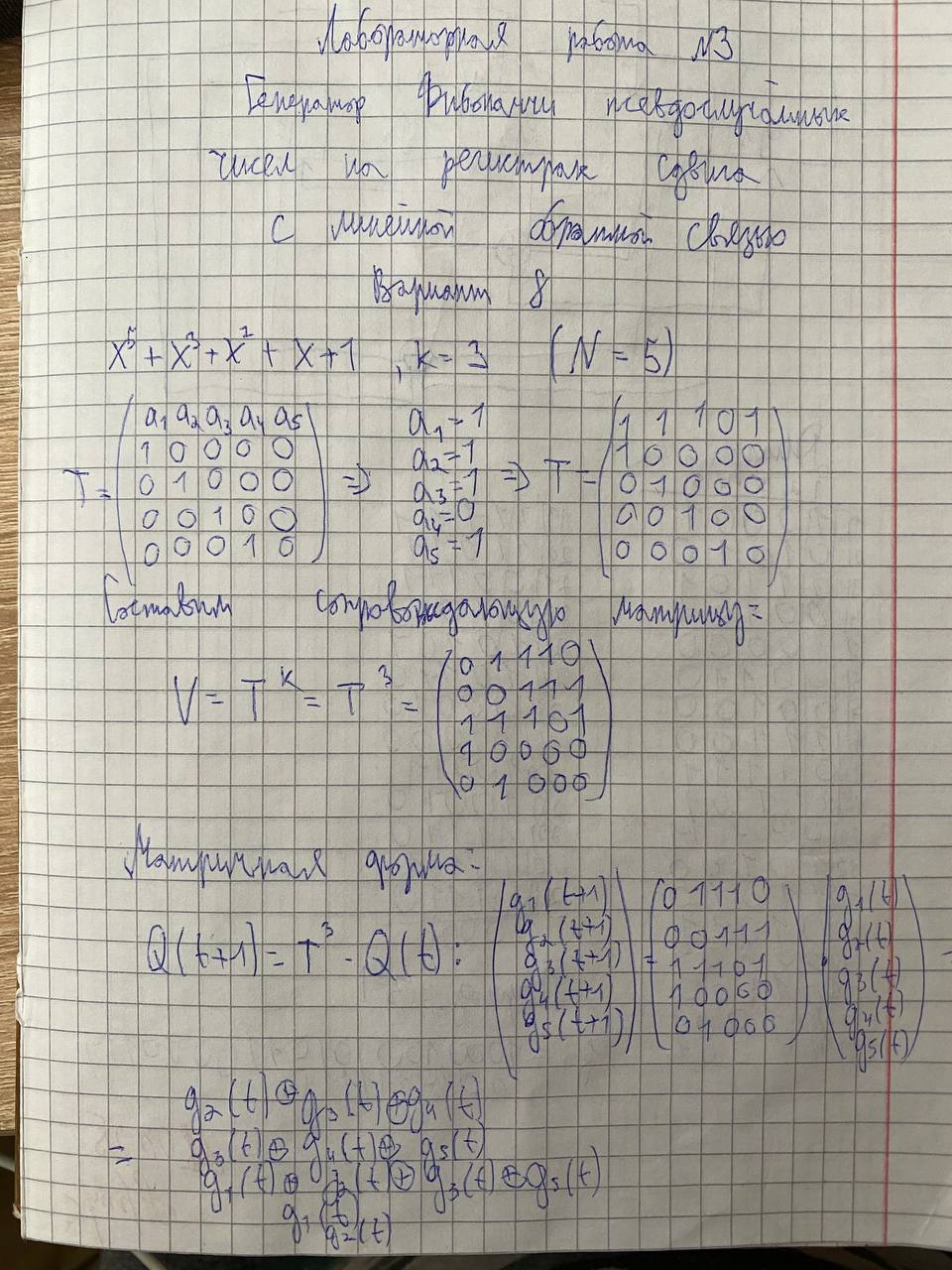


Рисунок 1 – Ручная отработка

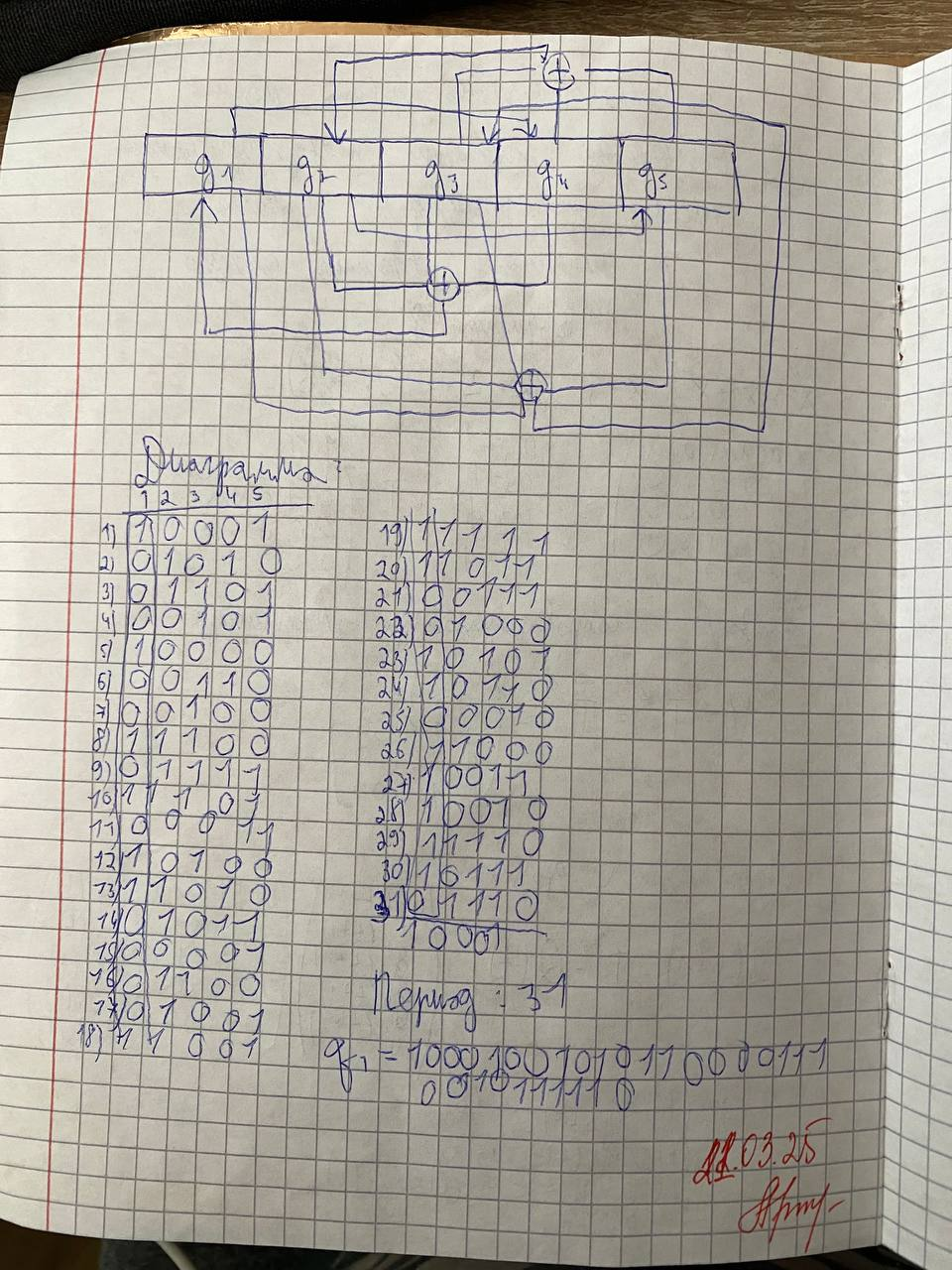


Рисунок 2 – Ручная отработка продолжение

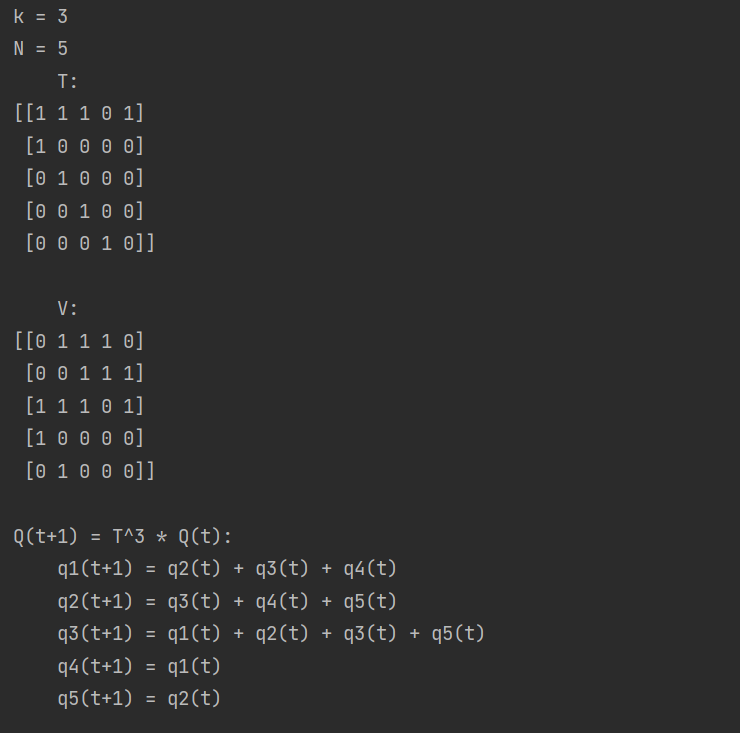


Рисунок 3 – Вывод в консоли

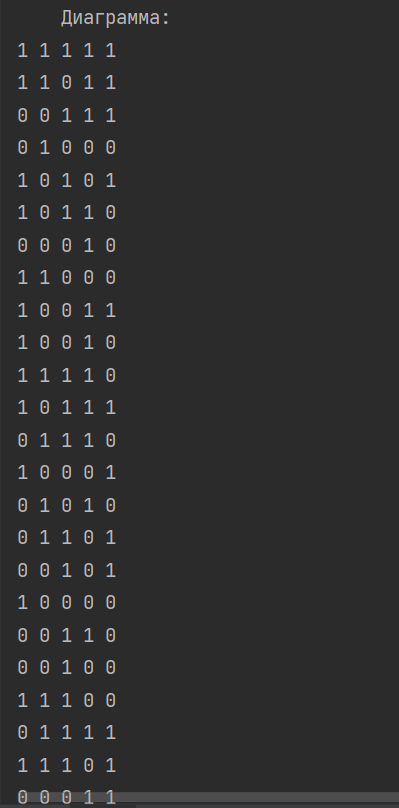


Рисунок 4 - Продолжение

Листинг кода:

import numpy as np  
from numpy.linalg import matrix\_power  
  
  
function = input('Введите функцию ->')  
k = int(input('Введите k ->'))  
start = input('Введите начально состояние регистра ->')  
X\_st = function.split('+')  
st = []  
for i in X\_st:  
 if i.split('\*\*')[0] != '1':  
 st.append(int(i.split('\*\*')[1]))  
st = sorted(st)  
N = st[-1]  
print(f'k = {k}\n'  
 f'N = {N}')  
  
T = np.array([[]])  
for i in range(N):  
 if i + 1 in st:  
 T = np.append(T, 1)  
 else:  
 T = np.append(T, 0)  
for i in range(N - 1):  
 T\_i = np.array([0]\*N)  
 T\_i[i] = 1  
 T = np.concatenate((T, T\_i), axis=0)  
else:  
 T = T.reshape(N, len(T)//N).astype('int')  
print(f'\tT:')  
print(T)  
  
V = matrix\_power(T, k)  
  
V\_new = []  
for i in range(len(V)):  
 V\_new.append([])  
 for y in range(len(V[i])):  
 V\_new[-1].append(V[i][y] % 2)  
V = np.array(V\_new)  
print(f'\n\tV:')  
print(V)  
  
Q\_t = []  
for i in range(len(V)):  
 Q\_t.append([])  
 for y in range(len(V[i])):  
 if V[i][y] == 1:  
 Q\_t[-1].append(y+1)  
  
print(f'\nQ(t+1) = T^{k} \* Q(t):')  
for i in range(len(Q\_t)):  
 string = ''  
 for y in range(len(Q\_t[i])):  
 string += f'q{Q\_t[i][y]}(t) + '  
print(f'\n\tДиаграмма:')  
start = [str(i) for i in start]  
print(' '.join(start))  
start\_save = start  
save = [start]  
while True:  
 start\_new = []  
 for i in range(len(Q\_t)):  
 num = 0  
 for y in range(len(Q\_t[i])):  
 num += int(start[Q\_t[i][y] - 1])  
 start\_new.append(str(num % 2))  
 start = start\_new  
 print(' '.join(start))  
 if start\_save == start:  
 break  
 save.append(start)  
print(f'Всего различных комбинаций {len(save)}\n')  
  
q\_N = ['']\*N  
for i in range(len(save)):  
 for y in range(N):  
 q\_N[y] += save[i][y]  
else:  
 print(f"q{number} = {q\_N[number - 1]}")

Вывод?