Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

ОТЧЕТ

по лабораторной работе № 1

“Методы генерации псевдослучайных чисел”

Выполнил: И.А. Григорик

Проверил:  И.Г. Алексеев

МИНСК 2023

**1 ЦЕЛЬ**

Изучить основные способы создания последовательностей случайных чисел с заданными законами распределения вероятности.

**2 ЗАДАНИЕ**

Написать приложение для моделирования генераторов псевдослучайных чисел. Использовать 64-битную арифметику целых чисел без знака.

1. Генератор на основе алгоритма Лемера  
2. Генератор на основе метода серединных произведений  
3. Генератор на основе регистра сдвига с обратными связями

Подобрать параметры для генераторов с целью получения наилучших результатов для каждого генератора (для выборок N = {10000, 500000, 100000000}).

Вывести гистограмму, матожидание, корреляцию и результаты 1-8 тестов NIST для лучшего случая.

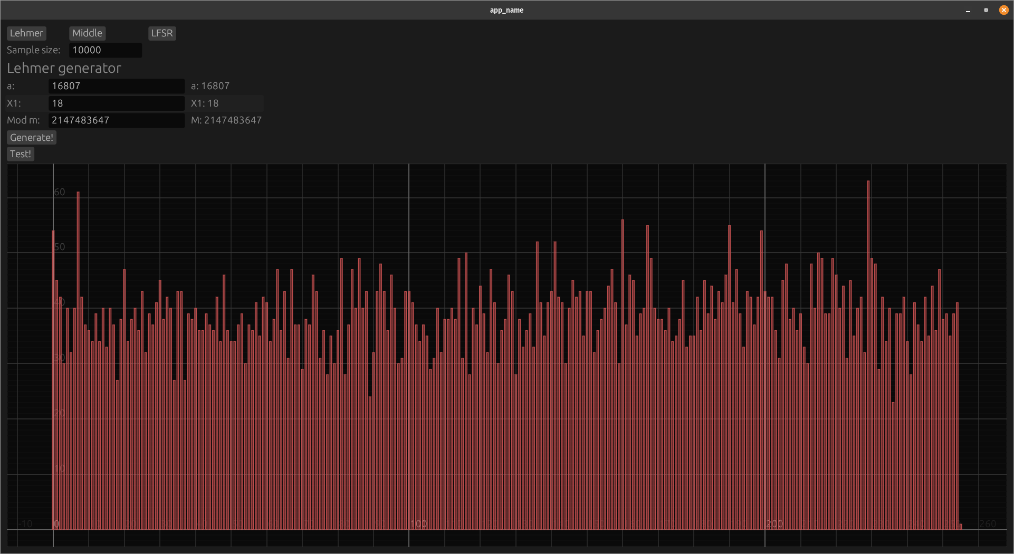
Сравнить полученные результаты с встроенным генератором.

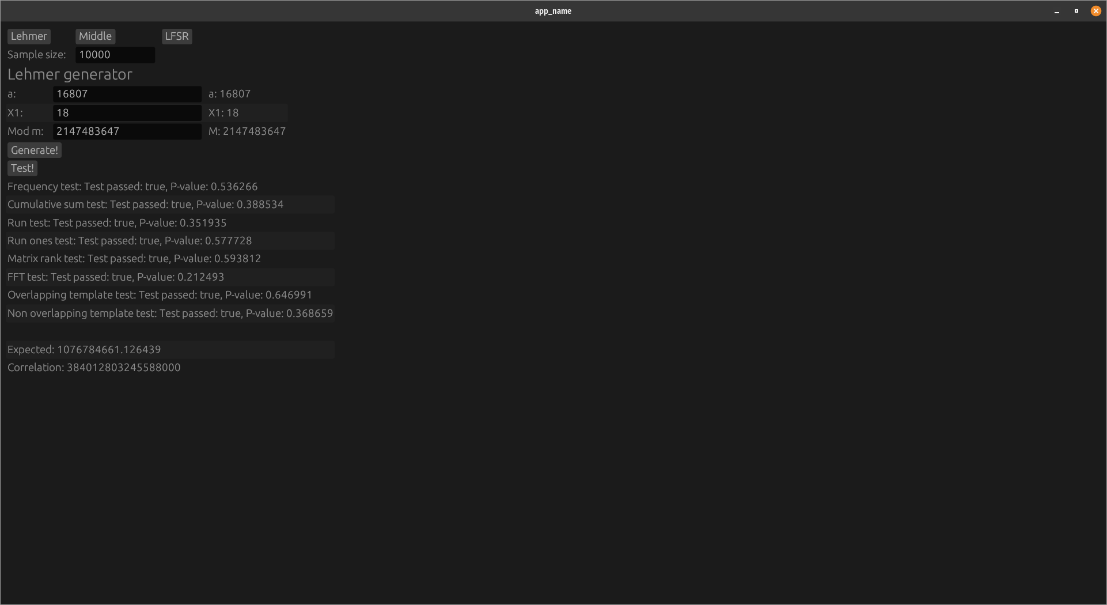
**3 ХОД РАБОТЫ**

**3.1 Генератор Лемера**

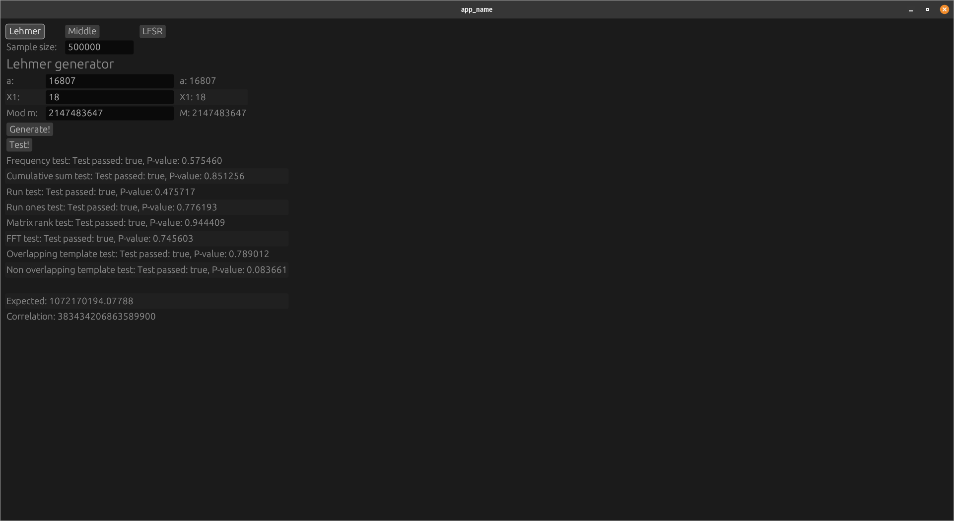
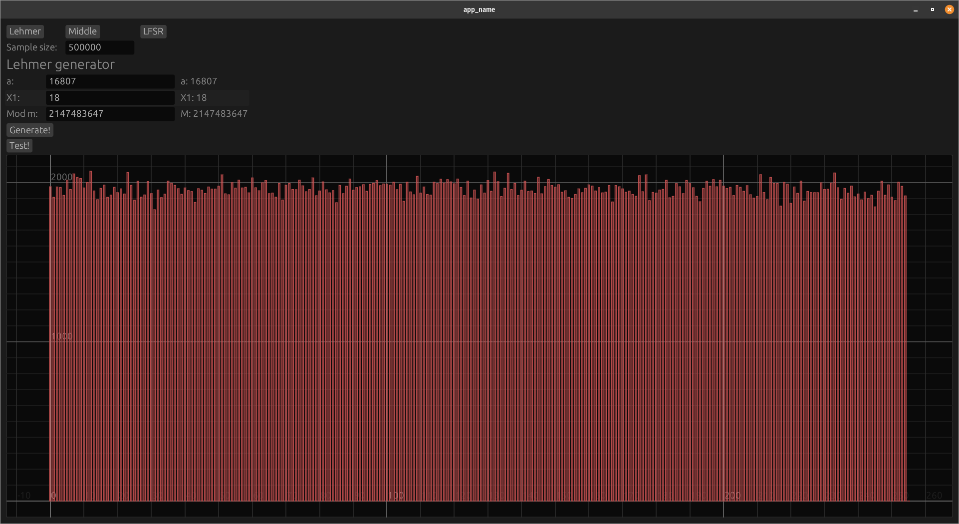
Генератор на основе алгоритма Лемера.

Генератор с выборкой равной n = 10000

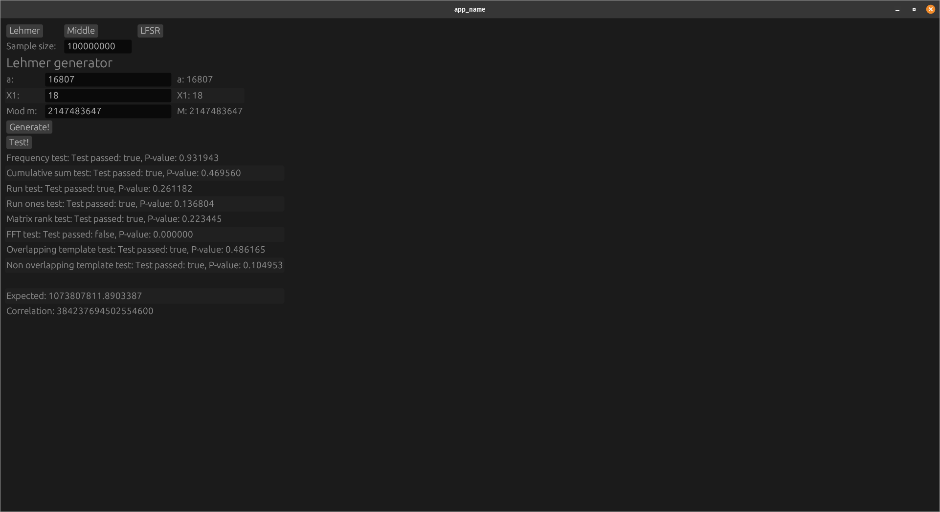
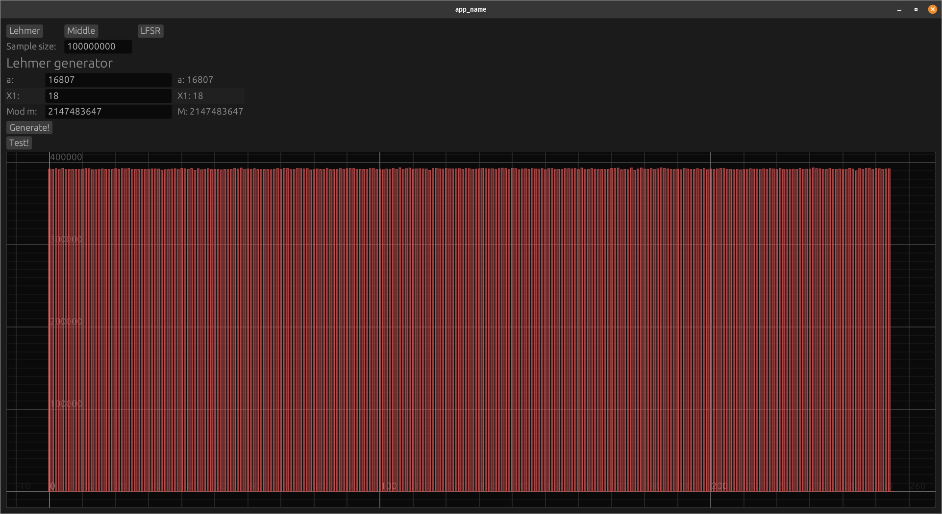




Генератор с выборкой равной n = 500000



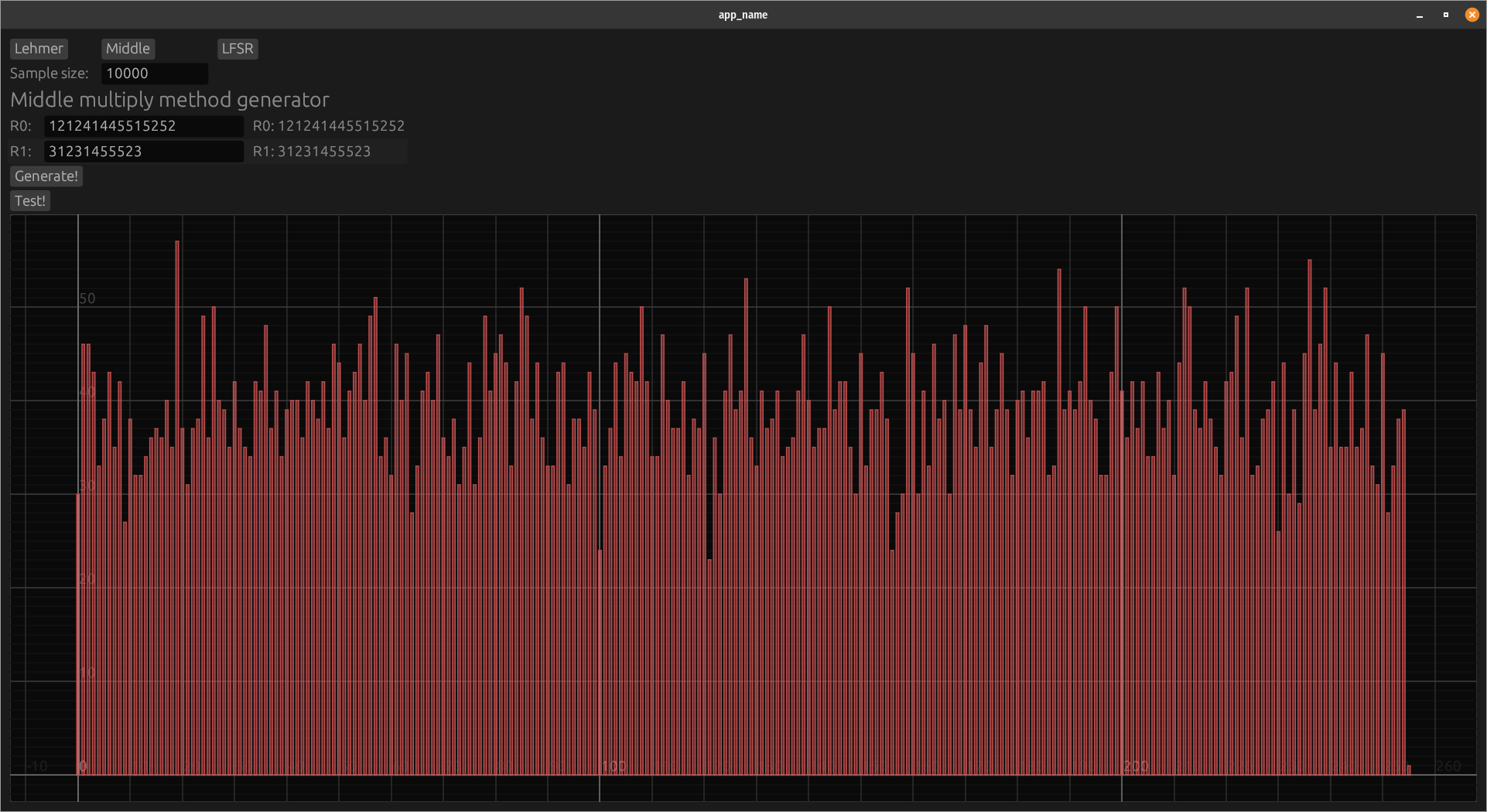
Генератор с выборкой равной n = 100000000

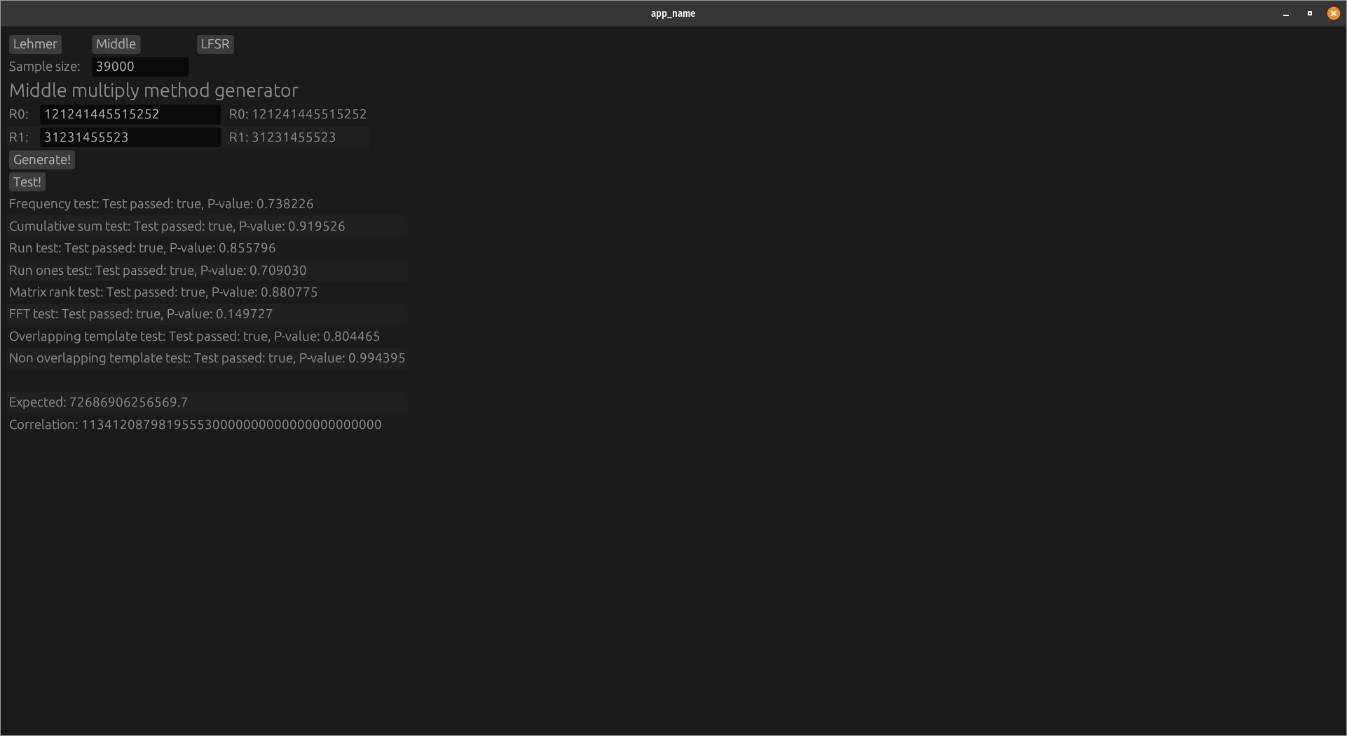


**3.2 Генератор серединных произведений**

Генератор на основе алгоритма серединных произведений.

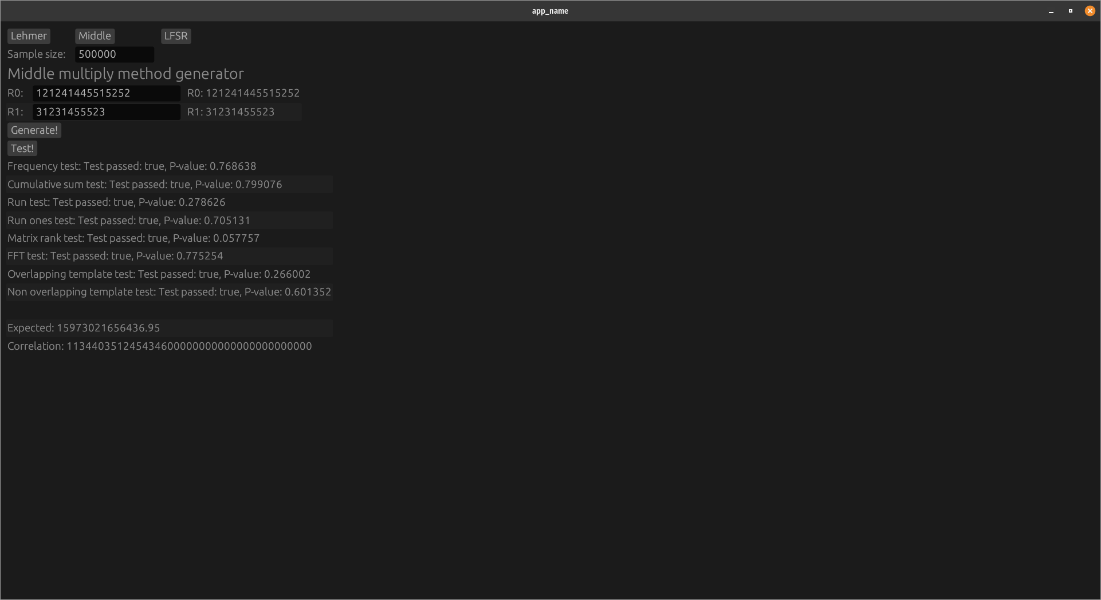
Генератор с выборкой равной n = 10000



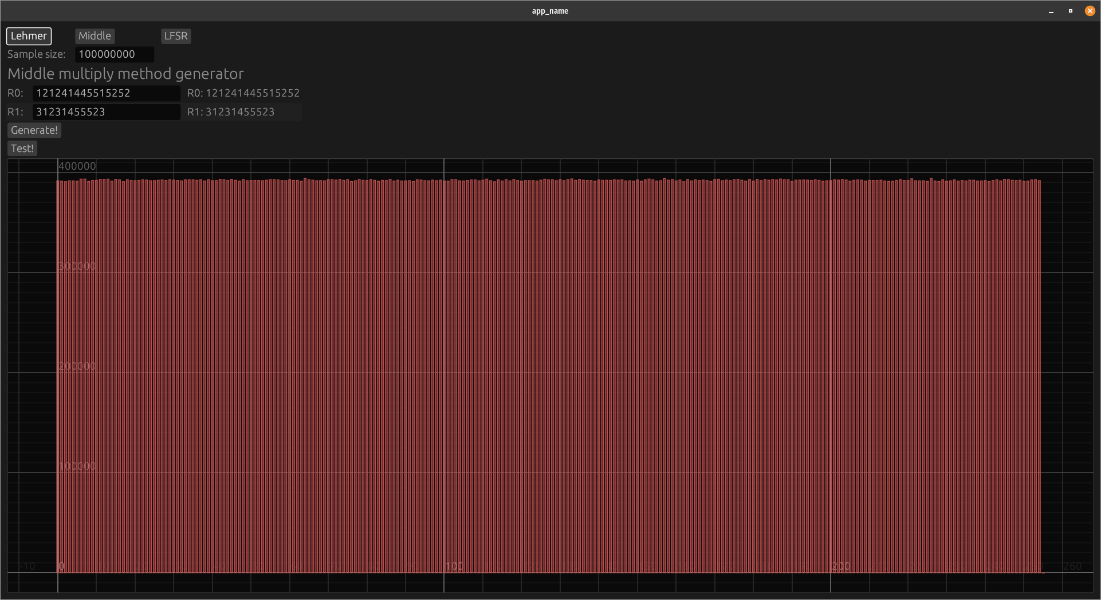


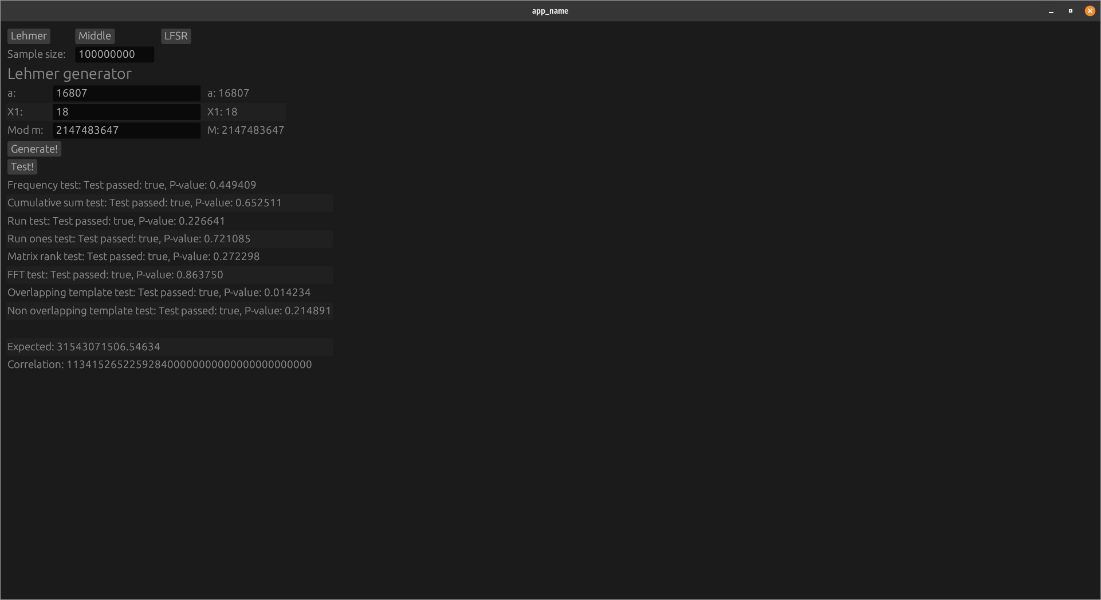
Генератор с выборкой равной n = 500000





Генератор с выборкой равной n = 100000000

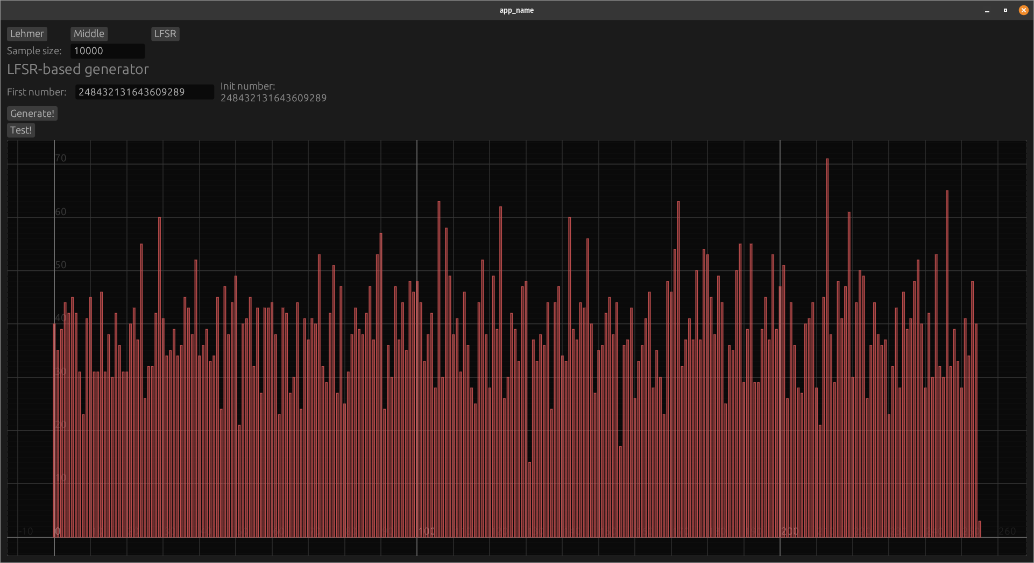


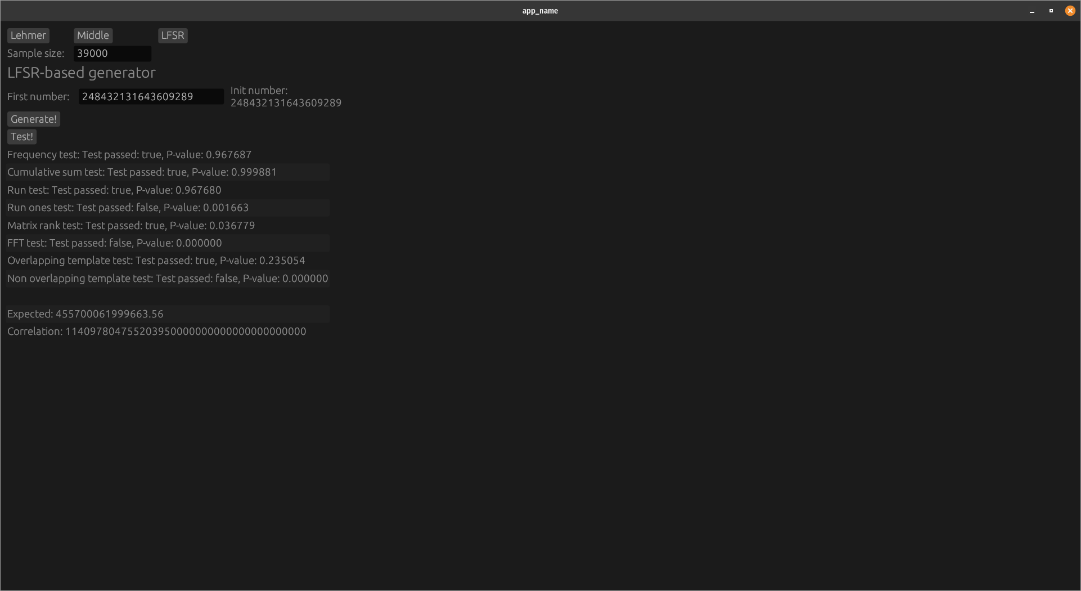


**3.3 Генератор, основанный на методе регистров обратной связи**

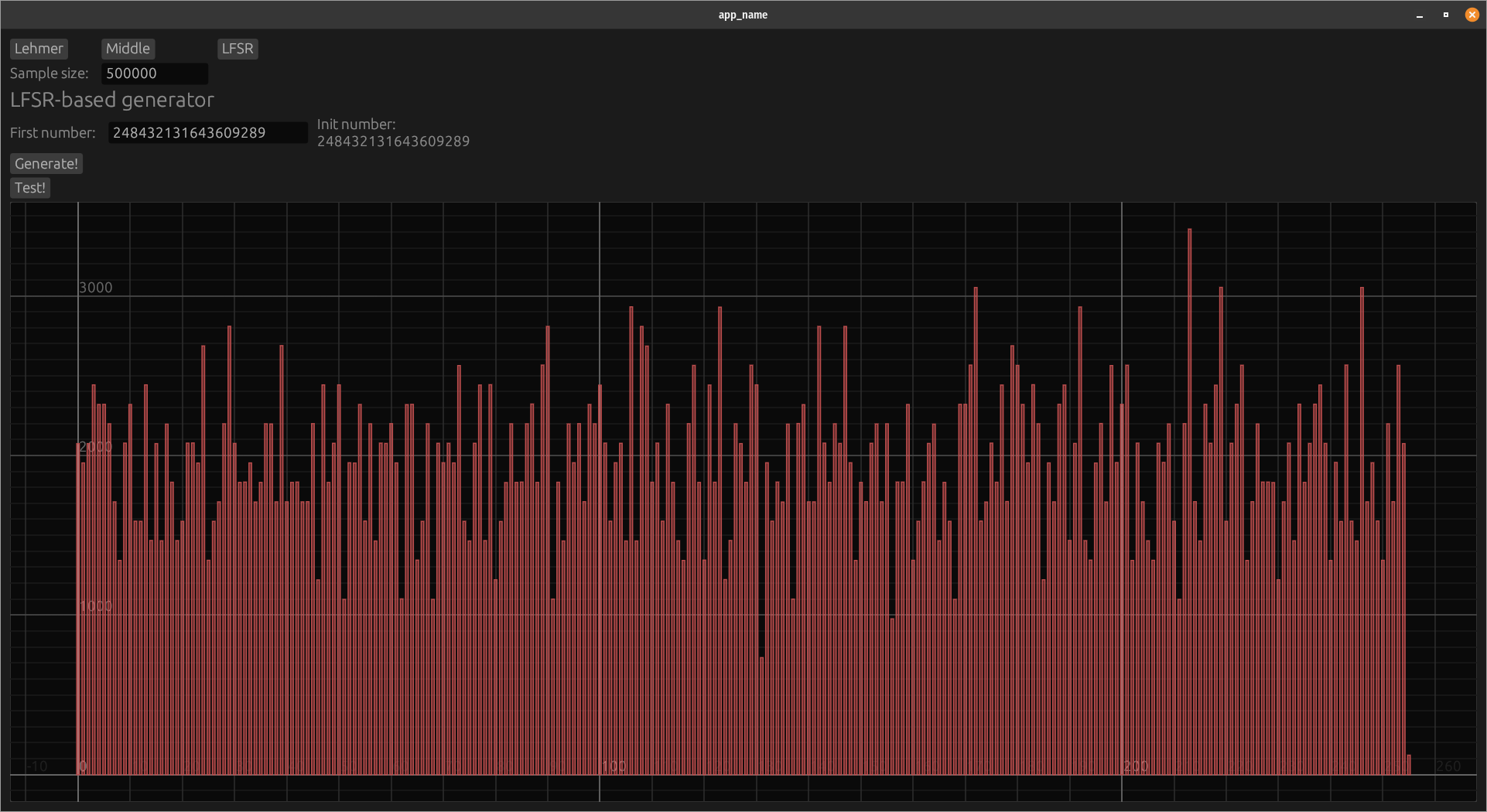
Генератор на основе алгоритма серединных произведений.

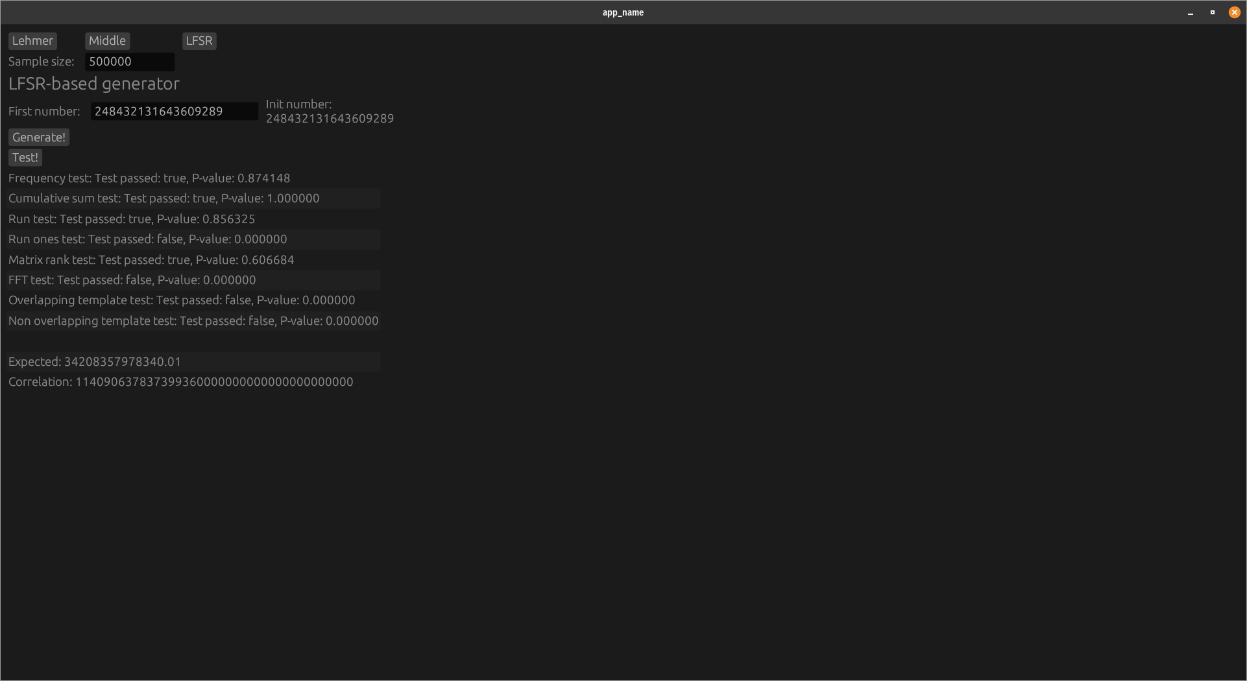
Генератор с выборкой равной n = 10000



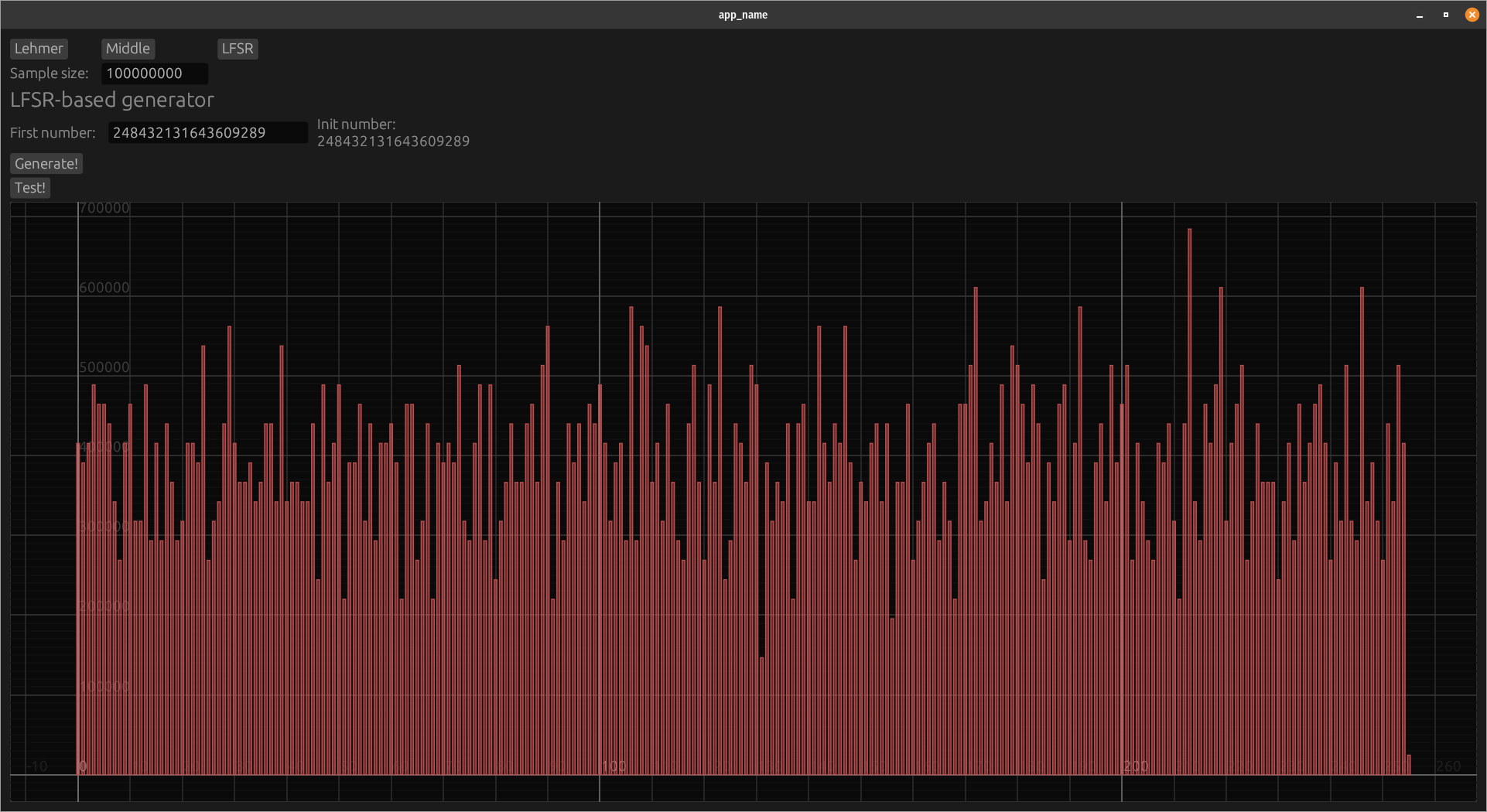


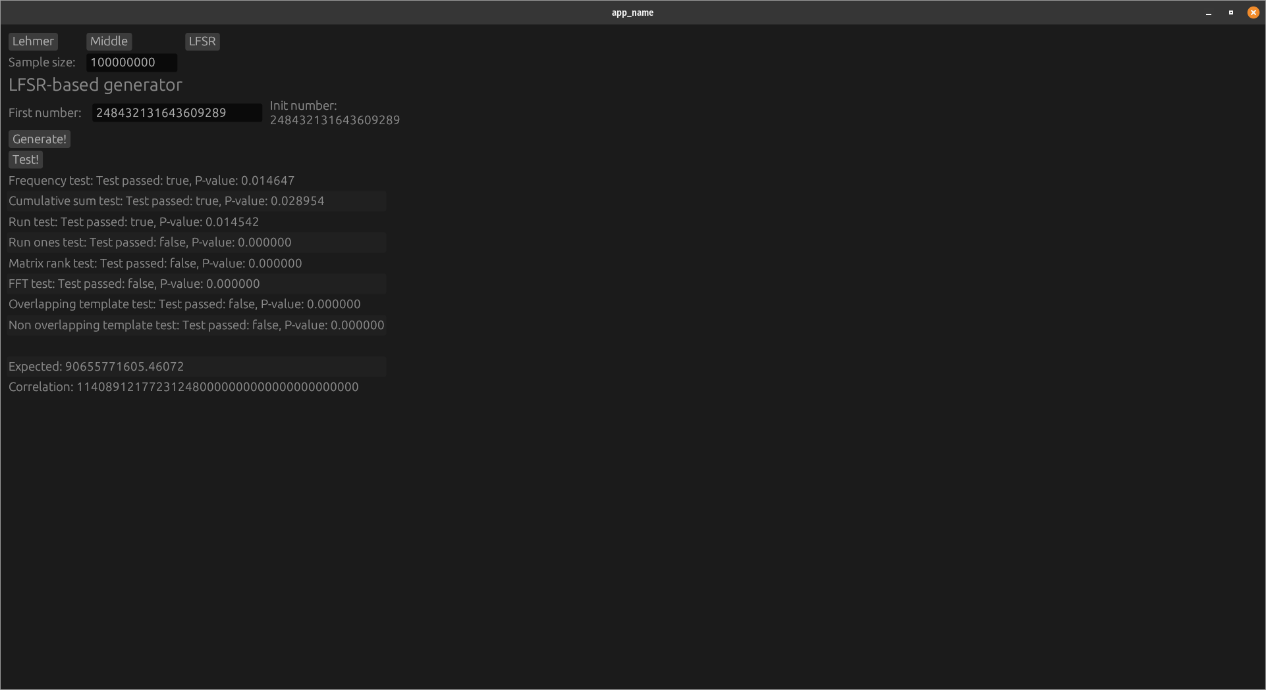
Генератор с выборкой равной n = 500000





Генератор с выборкой равной n = 100000000





**4 Листинг кода**

Данная лабораторная работа была выполнена на языке Rust

Генератор Лемера

fn generate\_lehmer(&mut self) {

let a = self.a\_buffer as u128;

let x1 = self.x1\_buffer as u128;

let m = self.m\_buffer as u128;

self.random\_numbers.push(x1 as u64);

for i in 1..self.count {

let t = a \* self.random\_numbers[i - 1] as u128;

let \_tmp = t % m;

self.random\_numbers.push(\_tmp as u64);

}

}

Генератор серединных произведений

fn generate\_middle(&mut self) {

let mut r0 = self.r0\_buffer as u128;

let mut r1 = self.r1\_buffer as u128;

let mask: u128 = 0xFFFFFFFFFFFFFFFF00000000; // mask to identify middle part of the number

for \_ in 0..self.count {

let mut new\_r = r0 \* r1;

new\_r &= mask;

new\_r >>= 32;

self.random\_numbers.push(new\_r as u64);

r0 = r1;

r1 = new\_r;

}

}

Генератор, основанный на методе регистров обратной связи

fn generate\_shift(&mut self) {

let mut num = self.shift\_buffer;

for \_ in 0..self.count {

// Identify two last bits bit

let b\_0 = num & 1;

let b\_1 = (num & 2) >> 1;

// Generate new last bit

let n\_bit = (b\_0 ^ b\_1) << 63;

// Shift our number and put the last bit

num >>= 1;

num |= n\_bit;

self.random\_numbers.push(num);

}

}