

Лабораторная работа № 2

Генерация последовательностей псевдослучайных чисел

Базовое задание (4 балла, дата сдачи $\leq 03.06.2021$).

Построить два линейных конгруэнтных генератора* с различными значениями модуля M :

1) $M < 103$, остальные параметры выбрать самостоятельно (**генератор 1**);

2) $M = p_i \times 2^{i+1} \times 18$, где i – ваш порядковый номер в списке группы (упорядоченном по алфавиту), p_i – i -ое нечетное совершенное число или i -ое простое число больше 1000; остальные параметры выбрать самостоятельно (с ограничениями: $a > 1$, $c > 1$) таким образом, чтобы период выходной последовательности генератора был максимальным (**генератор 2**).

По полученной выходной последовательности каждого генератора x_1, \dots, x_n длины $n > M$ построить диаграмму рассеяния, т.е. изобразить на плоскости множество точек $\{(x_1, x_2), (x_2, x_3), \dots, (x_{n-1}, x_n)\}$.

Дополнительные задания (принимаются при условии, что сдано основное задание, i -ое дополнительное задание принимается при условии, что сданы дополнительные задания $1, \dots, i-1$, $i = 2, 3, \dots$).

– **1** (2 балла, дата сдачи $\leq 18.03.2020$). На основе генераторов 1 и 2 построить два (различных) генератора Макларена-Марсальи (**генераторы 3 и 4**). Построить диаграммы рассеяния для $n > 2^{20}$ элементов выходной последовательности.

– **2** (2 балла, дата сдачи $\leq 18.03.2020$). Реализовать два регистра сдвига с линейной обратной связью: один – длины 5 с произвольным характеристическим многочленом, второй – длины 10 с примитивным характеристическим многочленом. Построить диаграммы рассеяния для $n > 2^{20}$ байтов выходной последовательности.

– **3** (1 балл, дата сдачи $\leq 11.03.2020$). На основе регистров сдвига из предыдущего задания построить сжимающий (прореживающий) генератор. Построить диаграмму рассеяния для $n > 2^{20}$ байтов выходной последовательности.

– **4** (1+5 баллов, дата сдачи $\leq 11.03.2020$). Реализовать программу, восстанавливающую характеристический многочлен регистра сдвига по выходной последовательности (длина регистра полагается известной).

*Линейный конгруэнтный генератор имеет вид:

$$x_{t+1} = (ax_t + c) \bmod M,$$

где x_1, x_2, \dots, x_n – выходная последовательность генератора длительности n , x_0 – начальное значение, a – множитель, c – приращение, M – модуль; $x_0, c, a, M \in \mathbb{N}$.