Лабораторная работа № 2

Генерация последовательностей псевдослучайных чисел

Базовое задание (4 *балла*, *дата сдачи* ≤ *24.03.2022*).

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

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

2) $M = p_i \times 2^i \times 18$, 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 $x_1,...,x_n$ длины $n > M$ построить диаграмму рассеяния, т.е. изобразить на плоскости множество точек $\{(x_1, x_2), (x_2, x_3) , ..., (x_{n-1}, x_n)\}$).

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

– 1 (2 *балла, дата сдачи* ≤ *17.03.2022*). На основе генераторов 1 и 2 построить два (различных) генератора Макларена-Марсальи (**генераторы 3 и 4**). Построить диаграммы рассеяния для $n > 2^{15}$ элементов выходной последовательности.

– 2 (2 *балла, дата сдачи* ≤ *17.03.2022*). 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 $n > 2^{15}$ байтов выходной последовательности, т.е. изобразить на плоскости множество точек $\{(x_1, x_2), (x_2, x_3) , ..., (x_{n-1}, x_n)\}$, где x_i – байт выходной последовательности генератора (число от 0 до 255).

– 3 (1 *балл, дата сдачи* ≤ *10.03.2022*). На основе регистров сдвига из предыдущего задания построить сжимающий (прореживающий) генератор. Построить диаграмму рассеяния для $n > 2^{15}$ байтов выходной последовательности.

– 4 (1+5 *баллов, дата сдачи* ≤ *10.03.2022*). Дешифровать файл с текстом (формат fb2), зашифрованный с помощью регистра сдвига с линейной обратной связью (файл прилагается, вариант вычисляется как $(N \bmod 12)+1$, где N – ваш номер в списке группы). Характеристический многочлен регистра сдвига.

$$f(x) = x^{16} + x^{15} + x^{12} + x^{10}+1.$$

Пример:
начальное состояние регистра (в двоичном представлении): 1000000000000001
байты открытого текста: 33 2E 2C 64 32 67 34 76
байты шифрующей гаммы: 80 01 19 5E F6 B5 AC 8A
байты шифртекста: B3 2F 35 3A C4 D2 98 FC

---

*Линейный конгруэнтный генератор имеет вид:

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

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