**Тема: «Методы генерации случайных чисел.»**

При исследовании различных динамических (изменяющихся во времени) систем часто используются имитационные модели. Согласно одному из определений, имитационная модель это определенный алгоритм, описывающий функционирование системы во времени, реализация которого осуществляется с помощью соответствующей машинной программы. При невозможности описать весь спектр воздействующих на систему факторов в модель вводится элемент случайности. Таким образом, для работы моделирующей программы необходима генерация случайных чисел. Компьютерная программа, работающая по определенному алгоритму, может генерировать только псевдослучайные (похожие на случайные) числа. Результаты работы различных алгоритмов проверяются статистическими тестами. Для генерации случайных чисел в программу подставляются случайным образом начальные условия. Для моделирования могут быть необходимы случайные величины с самыми разными характеристиками, но обычно, сначала генерируется базовая последовательность случайных чисел. Совокупность независимых, равномерно распределенных на отрезке [0,1] случайных величин Ri , (i=0,1…) называется последовательностью базовых случайных чисел. Существует несколько алгоритмов генерации базовой последовательности, рассмотрим некоторые из них.

Алгоритмы получения псевдослучайных чисел.

***Алгоритм середины квадратов Неймана***. Первый алгоритм для получения псевдослучайных чисел был предложен Дж. Фон Нейманом в 1951 г. Он называется методом середины квадратов.

Поясним его на ***примере***. Пусть задано случайно выбранное 4-значное число R0 = 0.9876. Возведя его в квадрат, получим 8-значное число R12= 0.97535376. Выбрав четыре средних цифры этого числа (они подчеркнуты), получим следующее псевдослучайное число: R1 = 0.5353. Повторив операцию возведения в квадрат R1 = 028654609 и процедуру выбора средних цифр числа R12 , получим очередное псевдослучайное число: R2 = 0.6546. Действуя аналогично, далее получим R22 = 0.42850116, R3 = 0.8501, R32 = 0.72267001,

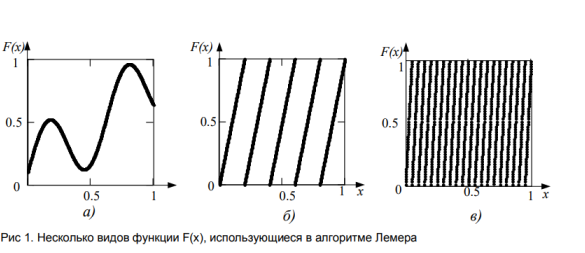
R4 = 0.2670, R42 = 0.07128900, R3 = 0.1289 и т.д. Таким образом, получен очень простой рекуррентный алгоритм генерирования псевдослучайных точек, который называется методом Неймана или методом серединных квадратов.

Для запуска (или инициализации) алгоритма достаточно задать некоторое произвольное начальное (или стартовое) число R0. Разным стартовым числам, вообще говоря, будут соответствовать разные последовательности чисел. Но этот алгоритм не оправдал себя: получалось больше чем нужно для равномерного распределения малых значений Ri . Кроме того, весьма часто последовательность случайных чисел оказывается слишком короткой, т.е. после некоторого Ri числа начинают повторяться. Но, что еще хуже, в последовательности может вообще отсутствовать случайность. Посмотрим, например, что будет, если в качестве начального числа выбрано R0=0.4500. В этом случае получим следующую последовательность: R02 = 0.20250000, R1 = 0.2500, R12 = 0.06250000, R2 = 0.2500, R22 = 0.06250000, R3 = 0.2500 и т.д., т.е. числа в последовательности вообще не меняются.

***Задача 1.*** Сгенерировать базовую последовательность N случайных чисел методом Неймана (срединных квадратов). N=6, R0=0,583.

***Задача 2.*** Сгенерировать базовую последовательность N случайных чисел модифицированным методом Неймана. N=6, R0=0,5836; R1=0,2176.

***Алгоритм Лемера***. Американский исследователь Д. Лемер предложил другой метод генерации базовой последовательности, представимый в виде формулы или реккурентного соотношения. Алгоритмы Лемера получения псевдослучайных чисел Ri+1 имеют достаточно простой вид: Ri+1 = F (Ri), i=0,1, … Начальное число R0 задано, а все последующие числа R1, R2, … вычисляются по одной и той же формуле. Заметим, что метод серединных квадратов, рассмотренный выше, также имеет аналогичный вид, но вместо аналитического задания функции y=F(x) была указана совокупность операций, которые надо проделать над аргументом x, чтобы получить значение y. Рассмотрим, какие требования необходимо предъявлять к функции F(x), чтобы последовательность удовлетворяла требованиям, предъявляемым к базовой последовательности, т.е. числам, равномерно распределенным на отрезке [0, 1] Рассмотрим пример, позволяющий понять, в чем состоит одна из основных трудностей при выборе F(x). Во-первых, аргумент и значение функции не должны выходить за пределы отрезка [0, 1]. Но это не все. Произвольная функция, например, график которой показан на рис.1 а) не подходит для генерации случайных чисел, поскольку все точки будут сконцентрированы на кривой, а настоящие случайные точки должны равномерно заполнять весь единичный квадрат. Таким свойством обладает, например, функция y = {g⋅x}, где g – очень большое число. Символ фигурных скобок {\*} означает дробную часть числа \*. На рис. 1,б-в) построен график функции y = {g⋅x}, при не очень больших числах g: они равны в случае б)g=5, и в) g=20.



***Задача 3.*** Сгенерировать базовую последовательность N случайных чисел при помощи алгоритма Лемера y={g⋅x}. N=5, R0=0,585; g=927.

***Конгруэнтный мультипликативный метод Лемера.*** В настоящее время, почти все стандартные библиотечные программы вычисления случайных базовых чисел основаны на конгруэтном методе, или методе сравнений. Два целых числа А и В конгруэнтны (сравнимы) по модулю m (где m—целое число) тогда и только тогда, когда существует такое целое число k, что А-В=km, т.е. если разность А-В делится на m и если числа А и В дают одинаковые остатки при делении на абсолютную величину числа m. Это определение записывается как А≡В(mod m) и читается «А конгруэнтно В по модулю m». Основная формула мультипликативного конгруэнтного метода имеет вид: Xi+1 = aXi(mod m), где а и m — неотрицательные целые числа. Согласно этому выражению, мы должны взять последнее случайное число Ri , умножить его на постоянный коэффициент а и взять модуль полученного числа 8 по m (т.е. разделить аXi на m и остаток считать как Xi+1). Поэтому для вычисления (или генерирования) последовательности Xi нам необходимы начальные значения X0, множитель а и модуль m. Выбираются а, X0 и m так, чтобы обеспечить максимальную длину (или, как говорят, период) неповторяющейся последовательности Xi и минимальную корреляцию между генерируемыми числами. В результате получается последовательность псевдослучайных чисел равномерно распределенных на интервале от 0 до m. Для того чтобы получить базовую последовательность, нужно разделить все числа последовательности Xi на m. Ri =Xi/m.

***Задача 4.*** Мультипликативным конгруэнтным методом сгенерировать базовую последовательность. a=265, m=129, X0=122.