***Практическое занятие № 8:***
***Алгоритмические генераторы случайных чисел***

**Цели занятия:**

- изучить основные алгоритмы генерации случайных чисел, имеющих равномерное распределение;
- приобрести навыки реализации основных алгоритмов генерации случайных чисел в среде MS Excel.

**Задание:**

- на основе лекционного материала произвести генерацию случайных чисел, используя следующие методы:
  - ***метод серединных квадратов;***
  - ***метод серединных произведений;***
  - ***метод перемешивания;***
  - ***линейный конгруэнтный метод.***
- найти для каждой полученной последовательности случайных чисел математическое ожидание и дисперсию и сделать выводы о степени соответствия полученной последовательности случайных чисел равномерному закону распределения.

**Метод серединных квадратов**

Имеется некоторое четырехзначное число R0. Это число возводится в квадрат и заносится в R1.

Далее из R1 берется середина (четыре средних цифры) — новое случайное число — и записывается в R0.

Затем процедура повторяется (рис. 1).

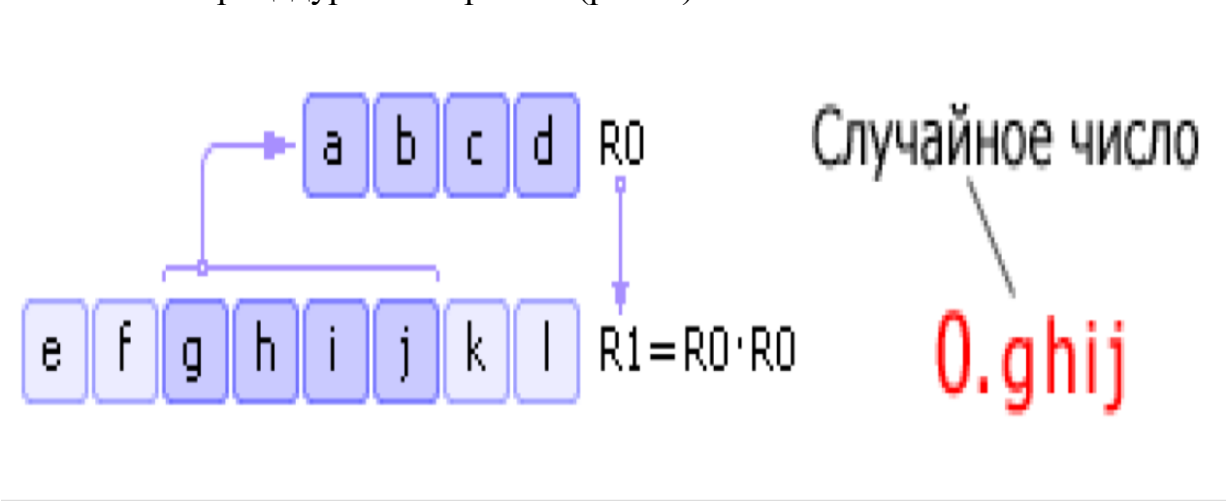


Рис. 1 - Метод серединных квадратов

**Недостатки метода**:

- если на некоторой итерации число ***R0*** станет равным нулю, то генератор вырождается, поэтому важен правильный выбор начального значения ***R0***;
- генератор будет повторять последовательность через ***M*n*** шагов (в лучшем случае), где n — разрядность числа ***R0***, ***M*** — основание системы счисления.

Описанный способ был предложен Джоном фон Нейманом и относится к 1946 году.

Реализация метода в среде MS Excel представлена на рис. 2.

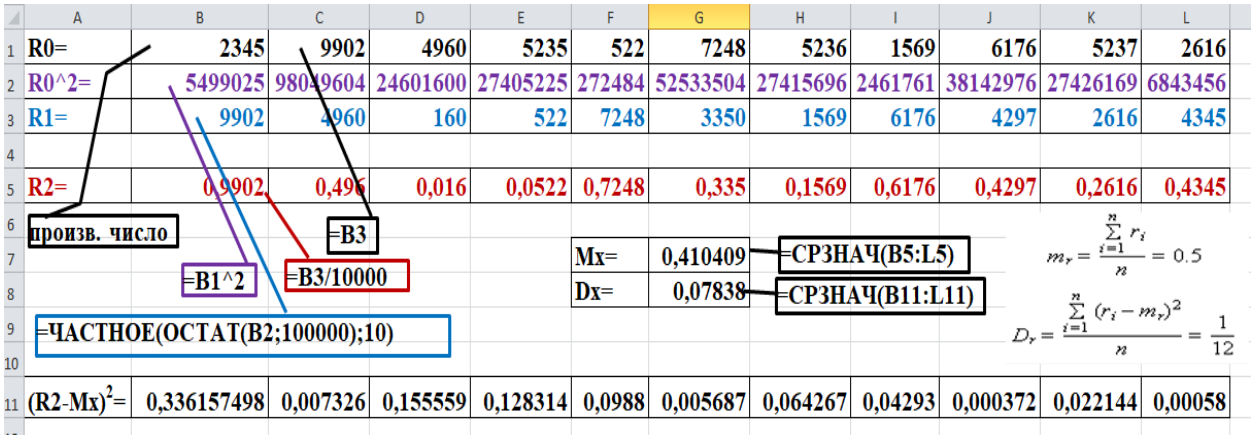


Рис. 2 – Реализация метода серединных квадратов

**Метод серединных произведений**

Число ***R0*** умножается на ***R1***, из полученного результата ***R2*** извлекается середина ***R2**** (это очередное случайное число) и умножается на ***R1***. По этой схеме вычисляются все последующие случайные числа (рис. 3).

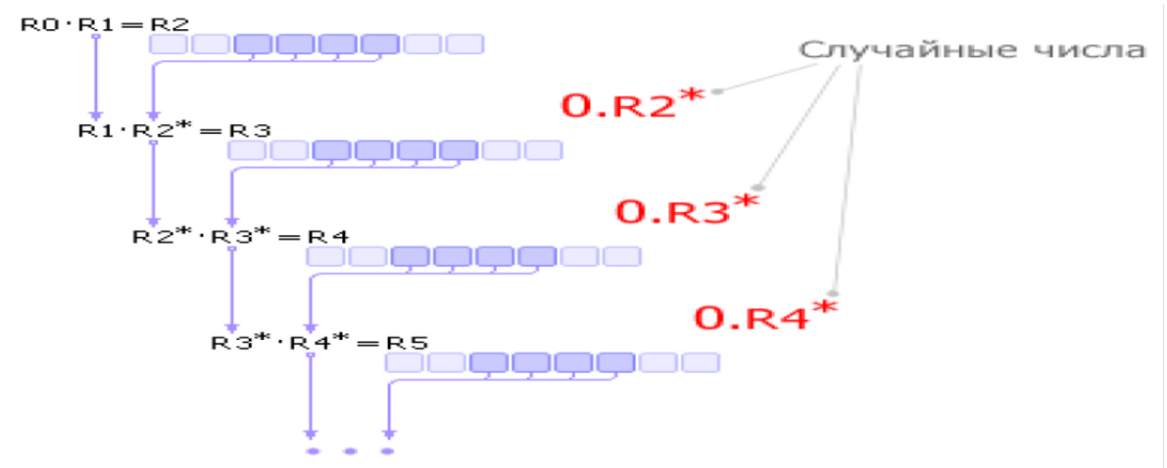


Рис. 3 - Метод серединных произведений

Реализация метода в среде MS Excel представлена на рис. 4.

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | R0= | 1087 | | =ЧАСТНОЕ(ОСТАТ(B3;100000);10)/10000 | | |
| 2 | R1= | 5678 | | Случайные Числа | | (R2-Mx)²= |
| 3 | R2=R0·R1= | 6171986 | | R2 | 0,7198 | 0,09032028 |
| 4 | R3=R1·R2*= | 40870244 | | R3 | 0,7024 | 0,08016448 |
| 5 | R4=·R2*·R3*= | 0,50558752 | | R4 | 0,5587 | 0,01944165 |
| 6 | R5=R3*·R4*= | 0,39243088 | | R5 | 0,243 | 0,03106994 |
| 7 | R6=R4*·R5*= | 0,1357641 | | R6 | 0,5764 | 0,02469088 |
| 8 | R7 | 0,1400652 | | R7 | 0,0065 | 0,17037632 |
| 9 | R8 | 0,0037466 | | R8 | 0,3746 | 0,00199511 |
| 10 | R9 | 0,0024349 | | R9 | 0,2434 | 0,03092908 |
| 11 | R10 | 0,09117764 | | R10 | 0,1177 | 0,09094245 |
| 12 | R11 | 0,02864818 | | R11 | 0,8648 | 0,19849995 |
| 13 | R12 | 0,10178696 | | R12 | 0,1786 | 0,05792044 |
| 14 | R13 | 0,15445328 | | R13 | 0,4453 | 0,00067773 |
| 15 | | | | Mx= | 0,419267 | |
| 16 | | | | Dx= | 0,066419 | |
| 17 | | | | | | |

=ЧАСТНОЕ(ОСТАТ(B4;100000);10)/10000

=ОСТАТ(ЧАСТНОЕ(B5*100000000;100);10000)/10000

Рис. 4 – Реализация метода серединных произведений

## Метод перемешивания

Используются операции циклического сдвига содержимого ячейки влево и вправо. Пусть в ячейке хранится начальное число ***R0***. Циклически сдвигая содержимое ячейки влево на 1/4 длины ячейки, получаем новое число ***R0****.

Точно так же, циклически сдвигая содержимое ячейки ***R0*** вправо на 1/4 длины ячейки, получаем второе число ***R0*****.

Сумма чисел ***R0**** и ***R0***** дает новое случайное число ***R1***. Далее ***R1*** заносится в ***R0***, и вся последовательность операций повторяется (рис. 5).

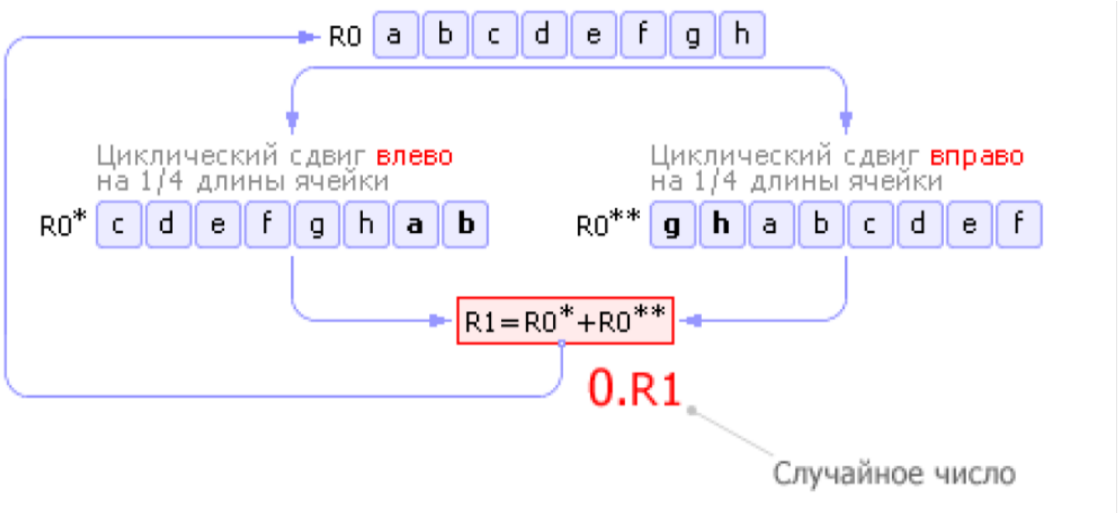


Рис. 5 - Метод перемешивания

Число, полученное в результате суммирования ***R0**** и ***R0*****, может не уместиться полностью в ячейке ***R1***. В этом случае от полученного числа должны быть отброшены лишние разряды.

На рисунке все ячейки представлены восемью двоичными разрядами.
Пусть ***R0**** = $10010001_2 = 145_{10}$, ***R0**** = $10100001_2 = 161_{10}$.
Тогда ***R0**** + ***R0**** = $100110010_2 = 306_{10}$.
Число 306 занимает 9 разрядов (в двоичной системе счисления), а ячейка ***R1*** (как и ***R0***) может вместить в себя максимум 8 разрядов.

Поэтому перед занесением значения в ***R1*** необходимо убрать один «лишний», крайний левый бит из числа 306, в результате чего в ***R1*** пойдет уже не 306, а $00110010_2 = 50_{10}$.

**Замечание**: в таких языках, как Паскаль, «урезание» лишних битов при переполнении ячейки производится автоматически в соответствии с заданным типом переменной.

Реализация метода в среде MS Excel представлена на рис. 6.

| | A | B | C | D | E | F | G | H | I | J | K | L |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | R0*= | | R0**= | | R1=R0*+R0**= | | 0,R1= | | (Mx-0,R1)^2= |
| 2 | R0= | 12345678 | | 34567812 | | 78123456 | | 112691268 | | 0,11269126 | | 0,110620698 |
| 3 | R0=R1= | 11269126 | | 26912611 | | 26112691 | | 53025302 | | 0,53025302 | | 0,007219027 |
| 4 | | 53025302 | | 2530253 | | 2530253 | | 5060506 | | 0,05060506 | | 0,155774749 |
| 5 | | 5060506 | | 6050605 | | 6050605 | | 12101210 | | 0,1210121 | | 0,105154963 |
| 6 | | 12101210 | | 10121012 | | 10121012 | | 20242024 | | 0,20242024 | | 0,058984827 |
| 7 | | 20242024 | | 24202420 | | 24202420 | | 48404840 | | 0,4840484 | | 0,001502356 |
| 8 | | 48404840 | | 40484048 | | 40484048 | | 80968096 | | 0,80968096 | | 0,132782113 |
| 9 | | 80968096 | | 96809680 | | 96809680 | | 193619360 | | 0,19361936 | | 0,063337185 |
| 10 | | 19361936 | | 36193619 | | 36193619 | | 72387238 | | 0,72387238 | | 0,077609168 |
| 11 | | 72387238 | | 38723872 | | 38723872 | | 77447744 | | 0,77447744 | | 0,108365582 |
| 12 | | 77447744 | | 44774477 | | 44774477 | | 89548954 | | 0,89548954 | | 0,202681283 |
| 13 | | | | =ОСТАТ(B2;100)*1000000+ЧАСТНОЕ(B2;100) | | | | | | Mx= | 0,44529 | Dx= 0,0930938 |
| 14 | | | | | | | | | | | | |
| 15 | =ОСТАТ(B2;1000000)*100+ЧАСТНОЕ(B2;1000000) | | | | | | | | | =ЕСЛИ(H2>10^8;ЧАСТНОЕ(H2;10);H2)/10^8 | | |
| 16 | | | | | | | | | | | | |
| 17 | | | | | | | | | | | | |

Рис. 6 – Реализация метода перемешивания

### Линейный конгруэнтный метод

Является одной из простейших и наиболее употребительных в настоящее время процедур, имитирующих случайные числа.

В этом методе используется операция **mod(x, y) .**

Каждое последующее случайное число рассчитывается на основе предыдущего случайного числа по следующей формуле:

$$r_{i+1} = mod(k*r_i + b, M).$$

где ***M*** — модуль (0 < M);

***k*** — множитель (0 ≤ k < M);

***b*** — приращение (0 ≤ b < M);

***r0*** — начальное значение (0 ≤ r0 < M).

Два целых числа A и B конгруэнтны (сравнимы) по модулю m (где m— целое число) тогда и только тогда, когда существует такое целое число ***k***, что

$$A-B=km,$$

т.е. если разность ***A-B*** делится на ***m*** и если числа ***A*** и ***B*** дают одинаковые остатки при делении на абсолютную величину числа ***m***.

Это определение записывается как $A \equiv B(mod\ m)$ и читается «A конгруэнтно B по модулю m».

Последовательность случайных чисел, полученных с помощью данной формулы, называется **линейной конгруэнтной последовательностью**.
Многие авторы называют линейную конгруэнтную последовательность при $b = 0$ **мультипликативным конгруэнтным методом,** а при $b \neq 0$ — **смешанным конгруэнтным методом**.

Для качественного генератора необходимо, чтобы число **M** было довольно большим, так как период не может иметь больше **M** элементов.

С другой стороны, деление, использующееся в этом методе, является довольно медленной операцией, поэтому для двоичной вычислительной машины логичным будет выбор $M = 2^N$, поскольку в этом случае нахождение остатка от деления сводится внутри ЭВМ к двоичной логической операции «AND».

Также широко распространен выбор наибольшего простого числа **M**, меньшего, чем $2^N$: в специальной литературе доказывается, что в этом случае младшие разряды получаемого случайного числа $r_{i+1}$ ведут себя так же случайно, как и старшие, что положительно сказывается на всей последовательности случайных чисел в целом.

Пример: $M = 2^{31} - 1$.

Одним из требований к линейным конгруэнтным последовательностям является как можно большая длина периода.

Длина периода зависит от значений ***M, k*** и ***b***.

***Линейная конгруэнтная последовательность, определенная числами M, k, b и $r_0$, имеет период длиной M тогда и только тогда, когда***:

- числа ***b*** и ***M*** взаимно простые;
- ***k – 1*** кратно ***p*** для каждого простого ***p***, являющегося делителем ***M***;
- ***k – 1*** кратно 4, если ***M*** кратно 4.

Пример: **M = 2N**

**k = 3 + 8 · q (или k = 5 + 8 · q)**

**b = 0**

**$r_0$ — нечетно**

Было установлено, что ряд псевдослучайных чисел, генерируемых на основе данных из примера, будет повторяться через каждые ***M/4*** чисел. Число ***q*** задается произвольно перед началом вычислений, однако при этом

следует иметь в виду, что ряд производит впечатление случайного при больших ***k*** (а значит, и ***q***).

Результат можно несколько улучшить, если ***b*** нечетно и $k = 1 + 4 \cdot q$ — в этом случае ряд будет повторяться через каждые ***M*** чисел.

После долгих поисков ***k*** исследователи остановились на значениях 69069 и 71365.

Пример: $M = 2^{31} - 1$

$k = 1\ 220\ 70\ 3\ 125$

$b = 7$

$r_0 = 7$

Генератор случайных чисел, использующий данные из примера, будет выдавать случайные неповторяющиеся числа с периодом, равным 7 миллионам.

Мультипликативный метод генерации псевдослучайных чисел был предложен Д. Г. Лехмером (D. H. Lehmer) в 1949 году.

Реализация метода в среде MS Excel представлена на рис. 7.

| | A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|---|
| 1 | $r_{i+1} = mod(k \cdot r_i + b, M)$ | | | | | | | | |
| 2 | M=2^31-1 = | 2147483647 | | k= | 1220703125 | | b= | 7 | |
| 3 | R0= | 7 | | приведение к 8 разрядам | | | Ri= | | (Mx-Ri)^2= |
| 4 | R1 | 2102470941 | | 210247094 | 21024709 | | 0,2102471 | | 0,048073 |
| 5 | R2 | 2095774539 | | 209577453 | 20957745 | | 0,2095775 | | 0,048367 |
| 6 | R3 | 293529164 | | 29352916 | 29352916 | | 0,2935292 | | 0,018489 |
| 7 | R4 | 534389740 | | 53438974 | 53438974 | | 0,5343897 | | 0,011001 |
| 8 | R5 | 856491030 | | 85649103 | 85649103 | | 0,856491 | | 0,18232 |
| 9 | R6 | 1964647199 | | 196464719 | 19646471 | | 0,1964647 | | 0,054306 |
| 10 | R7 | 2114713372 | | 211471337 | 21147133 | | 0,2114713 | | 0,047537 |
| 11 | R8 | 668376820 | | 66837682 | 66837682 | | 0,6683768 | | 0,057061 |
| 12 | R9 | 1155489451 | | 115548945 | 11554894 | | 0,1155489 | | 0,098566 |
| 13 | R10 | 1782919420 | | 178291942 | 17829194 | | 0,1782919 | | 0,063106 |
| 14 | R11 | 715592546 | | 71559254 | 71559254 | | 0,7155925 | | 0,081848 |
| 15 | R12 | 964039844 | | 96403984 | 96403984 | | 0,9640398 | | 0,285731 |
| 16 | | | | | | Mx= | 0,429502 | Dx= | 0,08303 |
| 17 | | | | | | | | | |
| 18 | | | | | | | | | |
| 19 | | | | | | | | | |

=ЕСЛИ(B4>10^8; ЧАСТНОЕ(B4;10);B4)

=ОСТАТ($E$2*B3+$H$2;$B$2)

=ЕСЛИ(D4>10^8; ЧАСТНОЕ(D4;10);D4)

=E4/10^8

Рис. 7 – Реализация линейного конгруэнтного метода