ТУСУР
TUSUR UNIVERSITY

Генерация случайных и псевдослучайных чисел, их свойства и тестирование.

Лекция 13

Доцент каф. АСУ: Суханов А.Я.

Введение

Случайные числа играют ключевую роль в моделировании, криптографии и численных методах.

•**Случайные числа:** генерируются физическими процессами.

•**Псевдослучайные числа:** вычисляются по алгоритмам, но имитируют случайность.

Цель презентации — изучить методы генерации псевдослучайных чисел, их свойства и подходы к тестированию.

Определение случайных и псевдослучайных чисел

ТУСУР
TUSUR UNIVERSITY

•**Случайные числа:** получены из физически непредсказуемых процессов, например, радиоактивного распада.

•**Псевдослучайные числа:** вычисляются по формулам и повторяемы.
Пример формулы: $\boldsymbol{x_n + 1 = (aX_n + c)\, mod\, m}$

Пример:

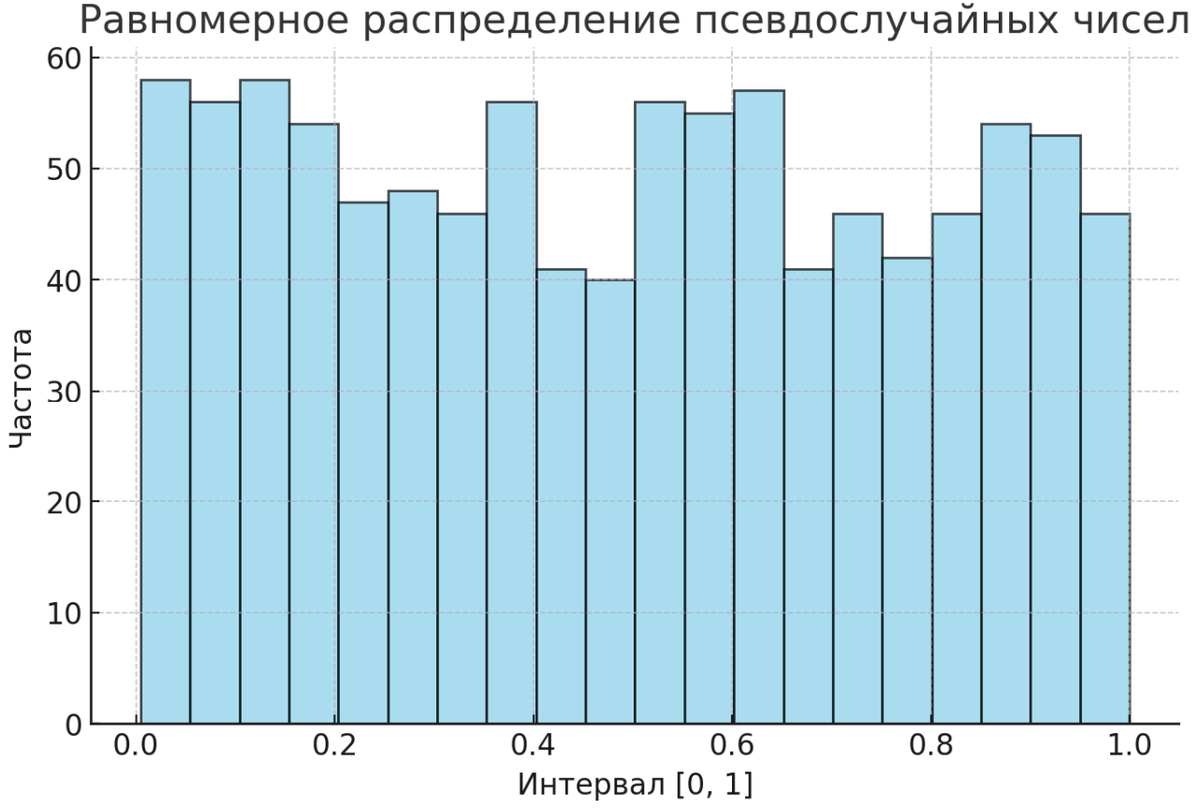
•$a = 5, c = 1, m = 9$, начальное значение $X0 = 3$.
Последовательность: 3,7,0,1,6,8,2,4,5.

Свойства псевдослучайных чисел

ТУСУР
TUSUR UNIVERSITY

- **Равномерное распределение:** числа должны быть равномерно распределены в заданном диапазоне.
- **Независимость:** каждое число не зависит от предыдущего.
- **Повторяемость:** для одинаковых начальных условий генератор всегда выдает одинаковую последовательность.
- **Большой период:** длина последовательности до её повторения.

Свойства псевдослучайных чисел



На диаграмме показано равномерное распределение псевдослучайных чисел на интервале $[0,1]$.
Гистограмма иллюстрирует, что числа распределены равномерно, что является одним из ключевых свойств.

Преимущества псевдослучайных чисел

- Небольшие вычислительные затраты.
- Возможность воспроизведения последовательностей.
- Универсальность для численных методов и моделирования.

Метод линейных вычетов

ТУСУР
TUSUR UNIVERSITY

Один из популярных алгоритмов генерации псевдослучайных чисел.

Формула:

$$Xn + 1 = (aXn + c) \ mod \ m$$

Пример:

•$a = 5, c = 1, m = 9$, начальное значение $X0 = 3$.
Последовательность: 3,7,0,1,6,8,2,4,5.

Метод линейных вычетов

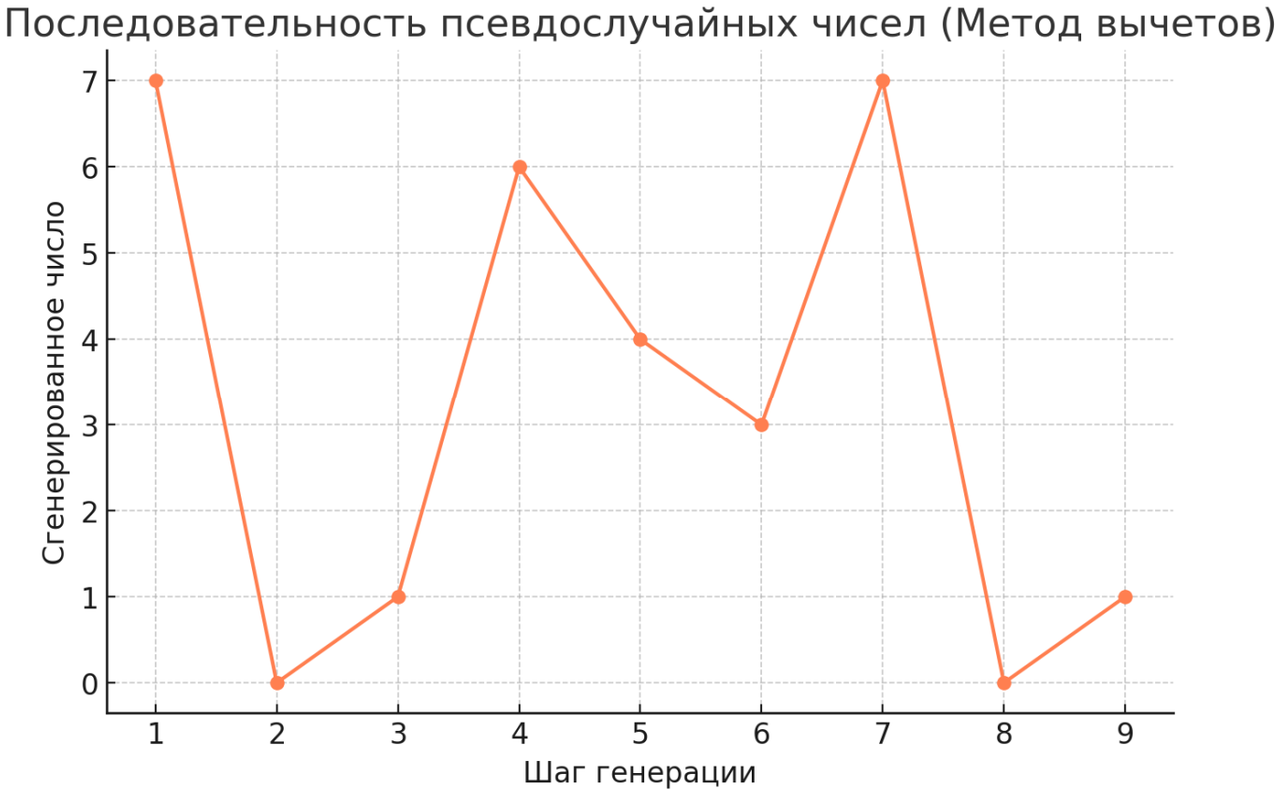


Диаграмма иллюстрирует последовательность чисел, сгенерированных методом линейных вычетов. Она показывает, как числа повторяются через период, что подчеркивает важность выбора параметров для получения длинных периодов.

Генерация случайных величин

ТУСУР
TUSUR UNIVERSITY

Пуассоновская случайная величина:

•Используется для моделирования событий, происходящих с постоянной интенсивностью.

•Вероятность $P(N = k) = \frac{\lambda^k e^{-\lambda}}{k!}$

Гауссовская случайная величина:

•Применяется для описания распределений вокруг среднего.

•Плотность вероятности: $f(x) = \frac{1}{\sqrt{2\Pi\sigma^2}} e^{\frac{-(x-\mu)^2}{2\sigma^2}}$

Методы моделирования гауссовской случайной величины

ТУСУР
TUSUR UNIVERSITY

- **Метод обратных функций:** сложен в реализации.

- **Метод Бокса-Мюллера:** позволяет быстро генерировать значения из гауссовского распределения:

$$x = \sqrt{-2InU_1}\, cos(2\pi U_2),$$

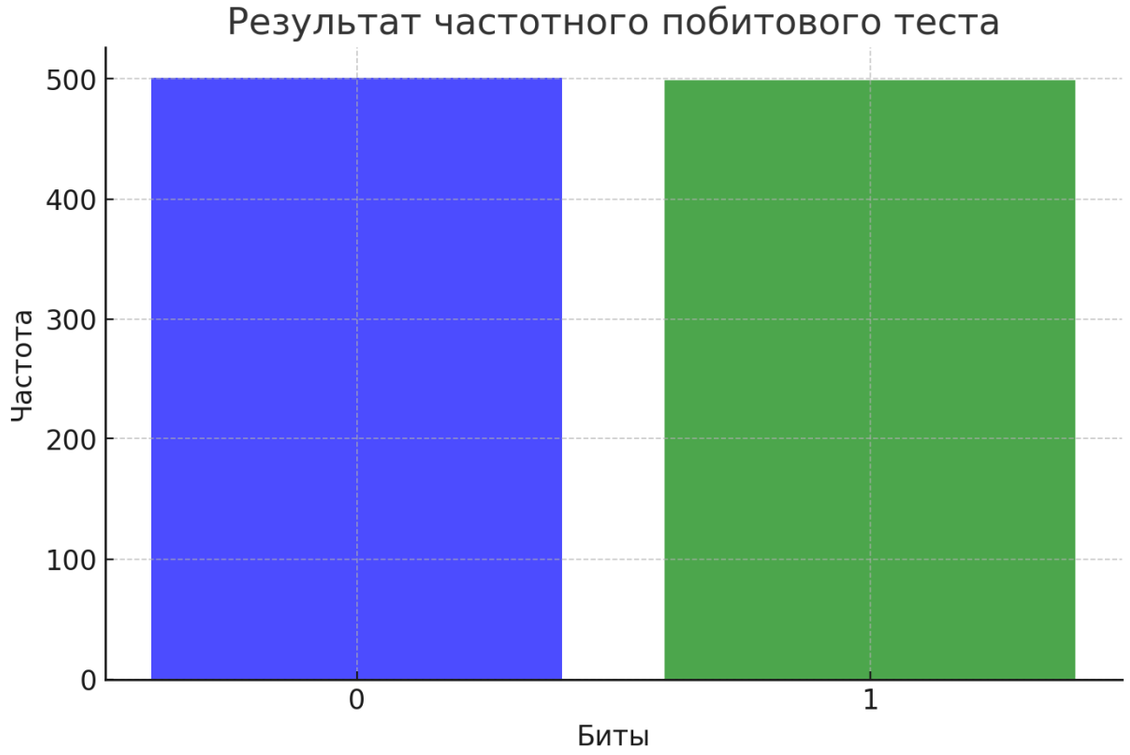
$$Y = \sqrt{-2\, ln\, U_1}\, sin(2\pi U_2)$$

Тестирование генераторов псевдослучайных чисел

Для проверки качества генераторов используются статистические тесты, оценивающие:

- Равномерность распределения.
- Независимость чисел.
- Отсутствие корреляций.

График показывает результаты частотного побитового теста, иллюстрируя равномерность распределения нулей и единиц в бинарной последовательности. Это важный критерий качества генератора случайных чисел.



Тесты DIEHARD

ТУСУР
TUSUR UNIVERSITY

Разработаны Джорджем Марсальей, проверяют свойства псевдослучайных последовательностей.
Примеры тестов:

1.Тест дней рождения: проверяет равномерность распределения точек на интервале.

2.Тест рангов матриц: анализирует линейную зависимость битов.

3.Тест на минимальное расстояние: оценивает расстояние между случайно размещёнными точками.

Тесты NIST

Пакет из 15 тестов, разработанный для проверки случайности последовательностей.

Примеры:

1.Частотный побитовый тест: равномерность числа нулей и единиц.

2.Тест на последовательности одинаковых битов: проверяет длины подряд идущих одинаковых символов.

3.Спектральный тест: оценивает периодические свойства последовательностей.

Диаграмма показывает результаты частотного блочного теста, где блоки проверяются на равномерность числа единиц. Это один из ключевых тестов NIST для оценки случайности.

Тесты Кнута

1.Проверка перестановок: анализирует порядок чисел в подпоследовательностях.

2.Тест на монотонность: проверяет увеличение и убывание подпоследовательностей.

3.Тест корреляции: оценивает взаимозависимость элементов последовательности.

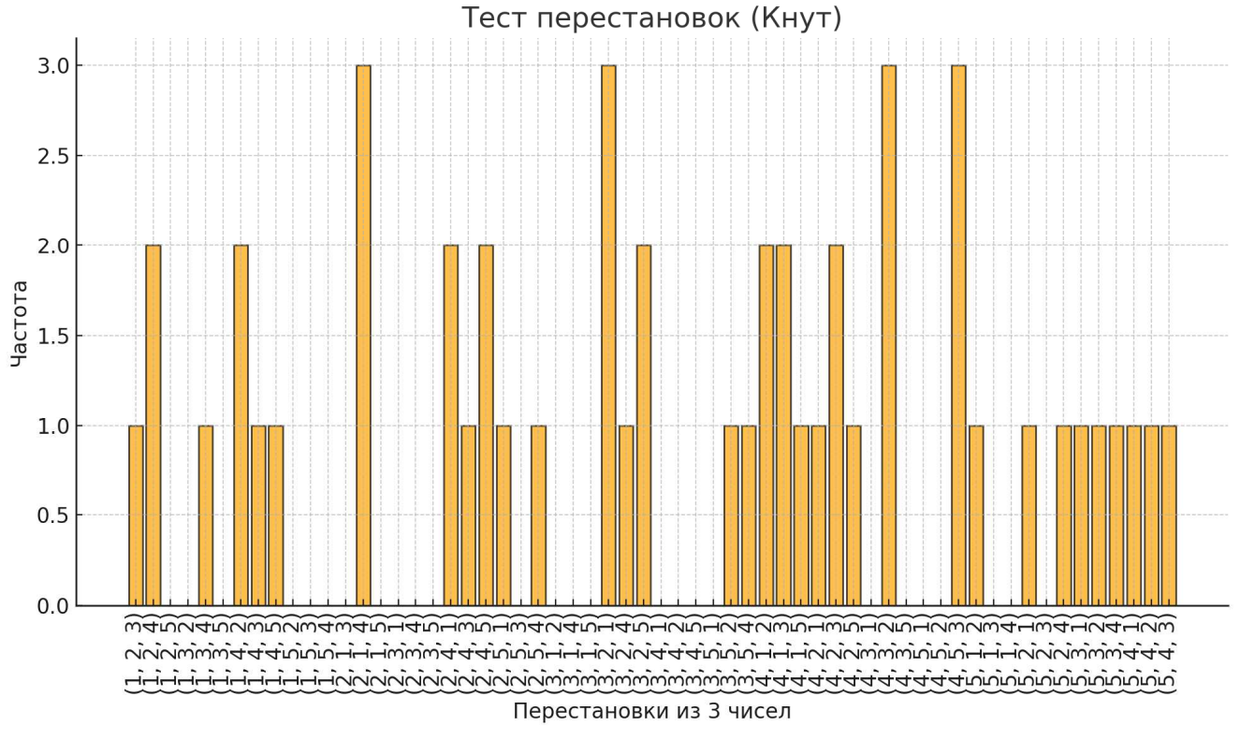


Диаграмма иллюстрирует результаты теста перестановок (Кнут), проверяющего, насколько равномерно распределены трёхэлементные подпоследовательности в случайной последовательности. Это помогает оценить качество генератора на уровне порядка чисел.

Преимущества и недостатки тестов

Преимущества:

•Высокая точность проверки.

•Возможность выявления скрытых зависимостей.

Недостатки:

•Высокая вычислительная сложность.

•Не всегда легко интерпретировать результаты.

Пример генерации и тестирования

Генерация 1000 чисел с использованием метода вычетов.
Тестирование:
1.Частотный побитовый тест.
2.Спектральный тест.
3.Тест на минимальное расстояние.

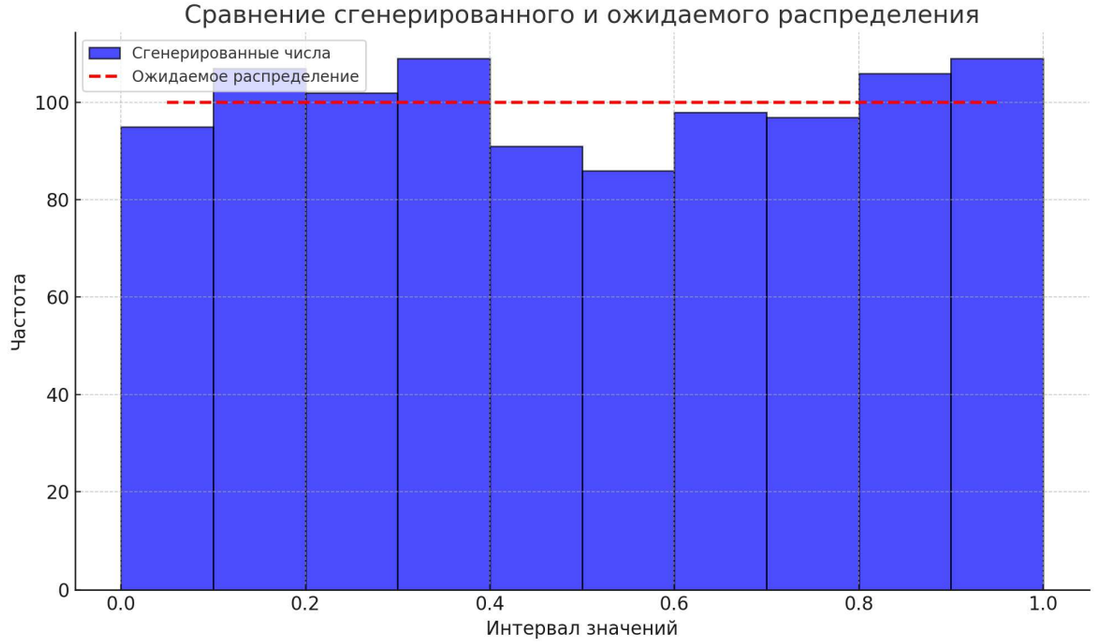


График иллюстрирует сравнение сгенерированного равномерного распределения случайных чисел с ожидаемым. Синие столбцы показывают частоту сгенерированных чисел в каждом интервале, а красная пунктирная линия представляет идеальное равномерное распределение.

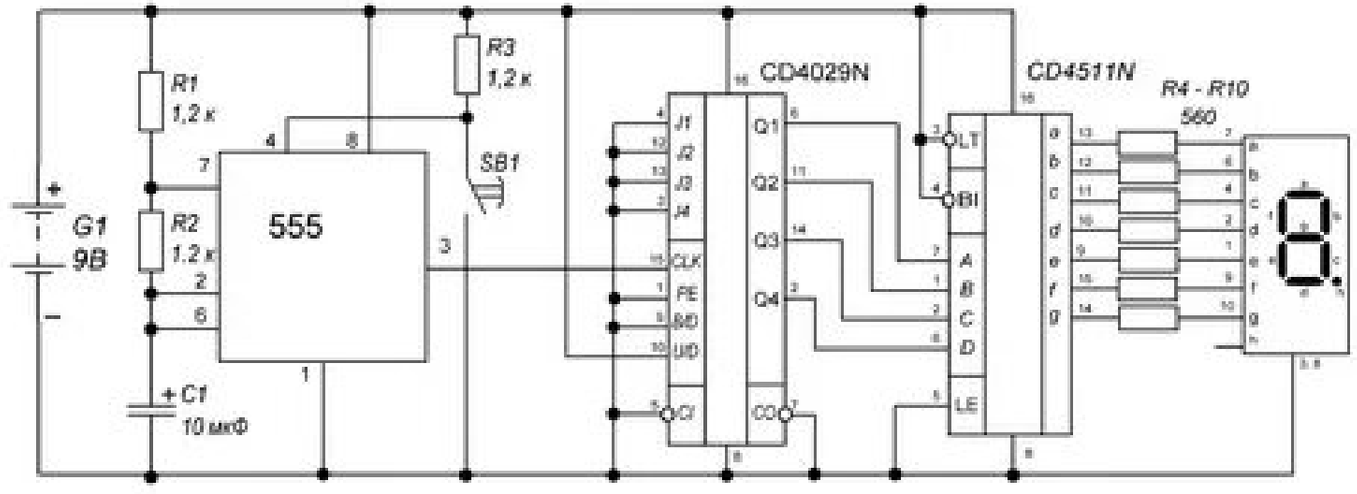
Применение генераторов псевдослучайных чисел

ТУСУР
TUSUR UNIVERSITY

- **Криптография:** генерация ключей.
- **Численные методы:** моделирование физических процессов.
- **Компьютерные игры:** случайные события и объекты.
- **Машинное обучение:** начальная инициализация весов.

Будущее генерации случайных чисел

- Аппаратные генераторы на основе квантовых эффектов.
- Улучшение алгоритмов псевдослучайности.
- Разработка более точных тестов качества.



Заключение

Генерация случайных и псевдослучайных чисел играет важную роль в различных областях, таких как моделирование, криптография и анализ данных. Псевдослучайные числа, несмотря на их алгоритмическую природу, могут успешно заменять истинно случайные числа в большинстве практических задач.
Ключевые выводы:

1.Для качественной генерации псевдослучайных чисел важны равномерность, независимость и большой период.

2.Разнообразные тесты, такие как **DIEHARD** и **NIST**, помогают оценить случайность последовательностей.

3.Технологии генерации постоянно совершенствуются, включая использование квантовых методов.

Эти методы открывают новые возможности для решения сложных задач, где важна случайность.

ТУСУР
TUSUR UNIVERSITY

СПАСИБО ЗА ВНИМАНИЕ!

г. Томск, ул. Вершинина, 47, офис 434

e-mail: aleksandr.i.sukhanov@tusur.ru

тел.: (3822) 70-15-36

tusur.ru