СРАВНИТЕЛЬНЫЙ АНАЛИЗ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Выполнила
студентка ОмГУ
ИМИТ
Заложнова
Вероника

ИСТОРИЯ ВОПРОСА

- В 1927 году Л. Типпетом впервые были опубликованы таблицы, содержащие свыше 40 000 случайных цифр.
- В 1939 году М. Ж. Кендалл и Б. Бабингтон-Смит использовали первый механический генератор случайных чисел для построения таблицы, содержащей 100 000 случайных цифр.
- В 1946 году американский математик Джон фон Нейман впервые предложил компьютерный алгоритм генерации случайных чисел.
- В 1955 году компания RAND Corporation опубликовала таблицы, содержащие 10^6 случайных цифр.
- С 1991 года в мире распространяется компакт-диск “The Marsaglia random number CDROM”, который сдержит 4,8 млрд. «истинно случайных» бит.

МЕТОДЫ ГЕНЕРИРОВАНИЯ СЛУЧАЙНЫХ ЧИСЕЛ

- Аппаратные ГСЧ – устройства, которые генерирует последовательность случайных чисел на основе измеряемых параметров протекающего физического процесса.
- Программные ГСЧ – различные алгоритмы, порождающие последовательности чисел, элементы которой в некотором смысле можно считать случайными.

МЕТОДЫ ГЕНЕРИРОВАНИЯ СЛУЧАЙНЫХ ЧИСЕЛ

Линейный конгруэнтный метод

$$X_{n+1} = (aX_n + c) \bmod m,$$

m – модуль, $m \geq 0$;

a – множитель, $0 \leq a < m$;

c – приращение, $0 \leq c < m$;

X_0 - начальное значение, $0 \leq X_0 < m$.

m, a, c, X_0 - целые числа.

Теорема

Линейная конгруэнтная последовательность, определенная числами m, a, c, X_0, имеет период длиной m тогда и только тогда, когда:

1. числа c и m взаимно простые;

2. a-1 кратно p для каждого простого p, являющегося делителем m;

3. a-1 кратно 4, если m кратно 4.

МЕТОДЫ ГЕНЕРИРОВАНИЯ СЛУЧАЙНЫХ ЧИСЕЛ

Аддитивный генератор Фибоначчи

$$X_n = \begin{cases} X_{n-a} - X_{n-b}, \text{если } X_{n-a} \geq X_{n-b}; \\ X_{n-a} - X_{n-b} + 1, \text{если } X_{n-a} < X_{n-b}, \end{cases}$$

где a и b – целые положительные числа, называемые лагами.

МЕТОДЫ ГЕНЕРИРОВАНИЯ СЛУЧАЙНЫХ ЧИСЕЛ

Генератор BBS

$X_{n+1} = X_n^2 \bmod M,$

где $M=pq$ – целое число Блюма,

p и q – большие простые числа,

$p \bmod 4=3$, $q \bmod 4=3$.

$X_0 = X^2 \bmod M$ – стартовое число генератора,

X – произвольное число взаимно простое с M.

ХОРОШИЙ ГЕНЕРАТОР ДОЛЖЕН ОБЛАДАТЬ СЛЕДУЮЩИМИ СВОЙСТВАМИ:

- Распределение получаемых последовательностей должно быть близко к равномерному
- Вычислительная эффективность
- Длинный период
- Повторимость
- Простота в реализации и в использования

ОСНОВНЫЕ ПРОВЕРКИ

ПРОВЕРКА НА РАВНОМЕРНОСТЬ

Критерий Пирсона

$$\chi^2 = \sum_{i=1}^{k} \frac{\left(N_i - \frac{N}{k}\right)^2}{\frac{N}{k}}$$

Если $\chi^2 < \chi^2_{\text{кр}}$ с заданным уровнем значимости, то данные эксперимента не противоречат гипотезе о равномерности распределения, иначе – противоречат.

k – количество интервалов на отрезке [0,1],

N_i – количество значений элементов последовательности, попавших в i-ый интервал,

N – общее число элементов сгенерированной последовательности.

ОСНОВНЫЕ ПРОВЕРКИ

ПРОВЕРКА НА НЕКОРРЕЛИРОВАННОСТЬ

Критерий Стьюдента

$$r_k = \frac{12}{N-k}\sum_{i=1}^{N-k}(x_i - 0.5)(x_{i+k} - 0.5)\ ,\ k = \mathrm{m};$$

$$t_k = \frac{r_k}{\sqrt{1 - r_k^2}}\sqrt{N-k-2}$$

Если $\forall k\ |t_k| < t_{\alpha,f}$, то гипотеза о незначительности коэффициента корреляции принимается, иначе – отвергается, где $t_{\alpha,f}$ - критическое значение, определяемой по таблице распределения Стьюдента при заданном уровне значимости α и $f = N-k-2$ степенях свободы.

ОСНОВНЫЕ ПРОВЕРКИ

ПРОВЕРКА НА РАВНОМЕРНОСТЬ

Математическое ожидание и дисперсия

$$M = \frac{1}{N}\sum_{i=0}^{N-1} x_i \qquad D = \frac{1}{N}\sum_{i=0}^{N-1} (x_i - M)^2$$

Для равномерно распределенных случайных чисел в интервале от 0 до 1 математическое ожидание и дисперсия должны быть следующими: $M = \frac{1}{2}, \mathrm{D} = \frac{1}{12}$.

ПЛАН ЭКСПЕРИМЕНТА

1. Выбрать параметры для рассмотренных ранее генераторов.

2. Применить основные проверки и графический тест.

3. По результатам отобрать наиболее удачные параметры для генераторов.

4. Посчитать приближенное значение числа π методом Монте-Карло при помощи выбранных генераторов.

5. Оценить результаты и сделать выводы.

ГРАФИЧЕСКИЙ ТЕСТ

Данный тест предназначен для определения зависимостей между элементами исследуемой последовательности.

Координату x в пикселе задает x_i элемент последовательности, координату y – x_{i+1}. Цвет пикселя задается в формате RGB:

R=$[x_{i+2} \cdot 255]$, G=$[x_{i+3} \cdot 255]$, B=$[x_{i+4} \cdot 255]$, $i = \overline{1, N-4}$.

ГЕНЕРАТОРЫ ДЛЯ ЭКСПЕРИМЕНТА

Линейный конгруэнтный генератор

1. $a=100$, $c=1$, $m=23211121111$, $X_0=6421$

2. $a=2416$, $c=374441$, $m=1771875$, $X_0=6421$

3. $a=1140671485$, $c=12820163$, $m=16777216$, $X_0=327680$

Генератор BBS

1. $p=3559$, $q=3571$, X=6421

2. $p=999983$, $q=999979$, X=6421

3. $p=20999939$, $q=20999999$, X=6421

Аддитивный генератор Фибоначчи

1. $a=2$, $b=1$ 2. $a=20$, $b=5$ 3. $a=97$, $b=33$

РЕЗУЛЬТАТЫ ПРОВЕРОК

КРИТЕРИЙ ПИРСОНА (С УРОВНЕМ ЗНАЧИМОСТИ 0.05)

Линейный конгруэнтный генератор

	$N = 10^3$	$N = 10^4$	$N = 10^5$	$N = 10^6$
$\chi^2_{\text{набл}}$ a=100, c=1, X_0=6421, m=23211121111	23.264	19.975	42.8452	40.5428
$\chi^2_{\text{набл}}$ a=2416, b=374441, m=1771875, X_0=6421	23.024	38.8974	14.8378	22.751
$\chi^2_{\text{набл}}$ a=1140671485, c=12820163, m=16777216, X_0=327680	18.368	52.6986	1664.6181	28340.5758
$\chi^2_{\text{кр}}$	35.1725	43.773	53.3835	62.8296

РЕЗУЛЬТАТЫ ПРОВЕРОК

КРИТЕРИЙ СТЬЮДЕНТА (С УРОВНЕМ ЗНАЧИМОСТИ 0.05)

	$N = 10^3$	$N = 10^4$	$N = 10^5$	$N = 10^6$
t_1	0.73793	2.2635	2.4403	9.84461
t_2	0.31974	3.0948	2.2978	9.82441
t_3	0.84826	3.5655	0.76954	10.7785
t_4	0.16952	4.9289	2.6332	10.9473
t_5	2.552	6.31	2.1875	9.83946
$t_{кр}$	1.6464	1.645	1.6449	1.6449

Линейный конгруэнтный генератор a=100, c=1, X_0=6421, m=23211121111

РЕЗУЛЬТАТЫ ПРОВЕРОК

КРИТЕРИЙ СТЬЮДЕНТА (С УРОВНЕМ ЗНАЧИМОСТИ 0.05)

	$N = 10^3$	$N = 10^4$	$N = 10^5$	$N = 10^6$
t_1	3.1906	1.3276	0.92056	0.53637
t_2	3.806	1.3501	0.20787	0.18947
t_3	3.9321	1.5671	1.1341	0.26935
t_4	4.1682	0.43863	1.3464	0.14361
t_5	4.295	0.58508	1.3981	0.15799
$t_{кр}$	1.6464	1.645	1.6449	1.6449

Линейный конгруэнтный генератор a=2416, b=374441, m=1771875, X_0=6421

РЕЗУЛЬТАТЫ ПРОВЕРОК

КРИТЕРИЙ СТЬЮДЕНТА (С УРОВНЕМ ЗНАЧИМОСТИ 0.05)

	$N = 10^3$	$N = 10^4$	$N = 10^5$	$N = 10^6$
t_1	1.5678	1.219	10.8258	36.8262
t_2	2.9348	0.17476	11.2871	39.8524
t_3	2.1847	0.35187	7.14663	25.6378
t_4	1.4668	1.0797	16.5142	56.7847
t_5	1.7228	2.8127	20.9348	70.7454
$t_{кр}$	1.5678	1.219	10.8258	36.8262

Линейный конгруэнтный генератор a=1140671485, c=12820163, m=16777216, X_0=327680

РЕЗУЛЬТАТЫ ПРОВЕРОК

ОТКЛОНЕНИЕ МАТЕМАТИЧЕСКОГО ОЖИДАНИЯ

Линейный конгруэнтный генератор

	$N = 10^3$	$N = 10^4$	$N = 10^5$	$N = 10^6$
a=100, c=1, X_0=6421, m=23211121111	0.0047682	0.0053144	0.0013999	9.8974e-05
a=2416, b=374441, m=1771875, X_0=6421	0.013258	0.0021609	0.0014786	1.7155e-05
a=1140671485, c=12820163, m=16777216, X_0=327680	0.0077135	0.002895	0.0004519	0.00073743

РЕЗУЛЬТАТЫ ПРОВЕРОК

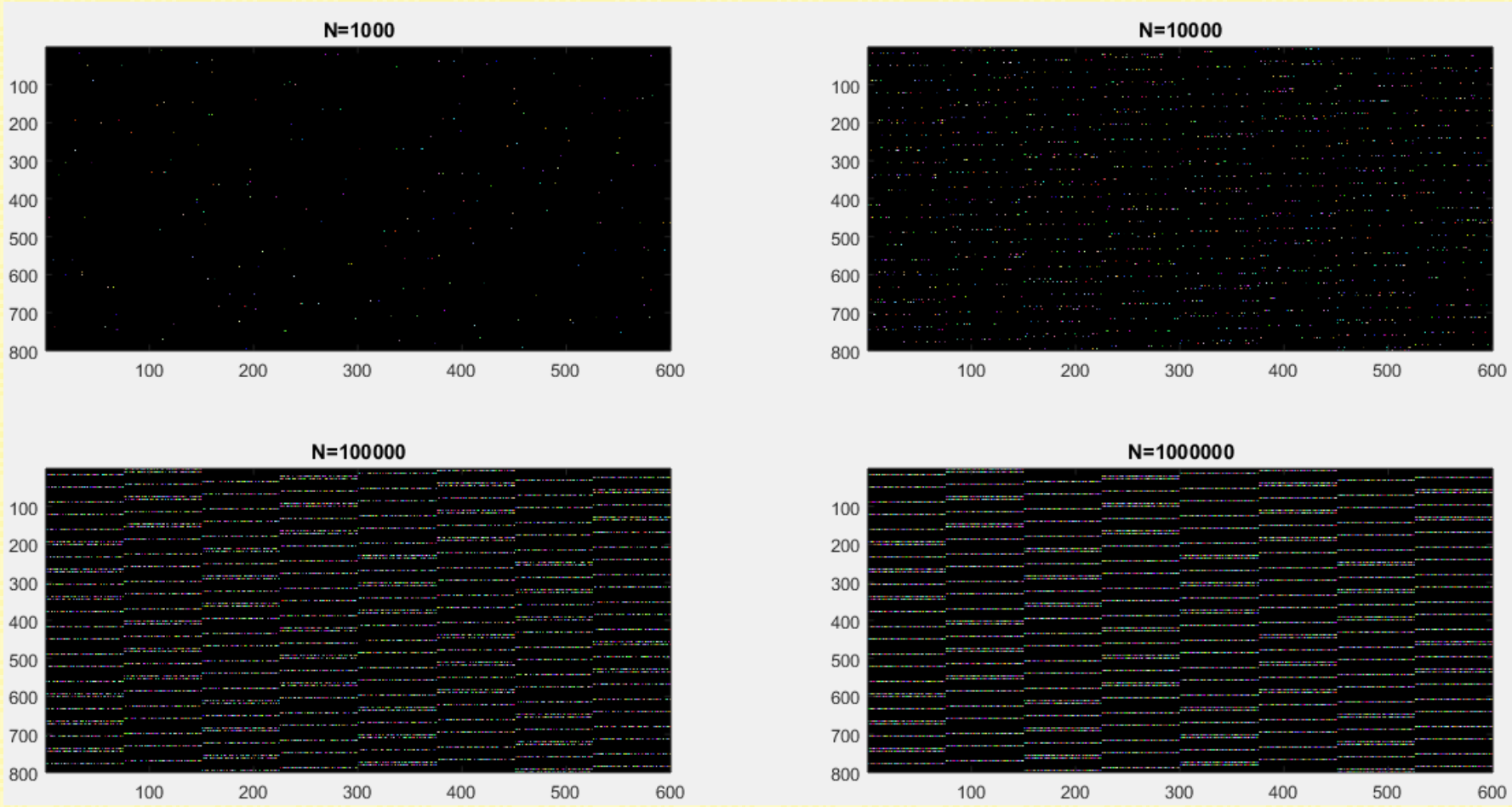
ОТКЛОНЕНИЕ ДИСПЕРСИИ

Линейный конгруэнтный генератор

	$N = 10^3$	$N = 10^4$	$N = 10^5$	$N = 10^6$
a=100, c=1, X_0=6421, m=23211121111	0.00030841	8.1906e-05	2.4785e-05	1.4291e-05
a=2416, b=374441, m=1771875, X_0=6421	0.0013205	0.00081446	1.4623e-06	2.2053e-05
a=1140671485, c=12820163, m=16777216, X_0=327680	0.0013461	0.0004676	6.9702e-06	1.3934e-05

РЕЗУЛЬТАТЫ ПРОВЕРОК

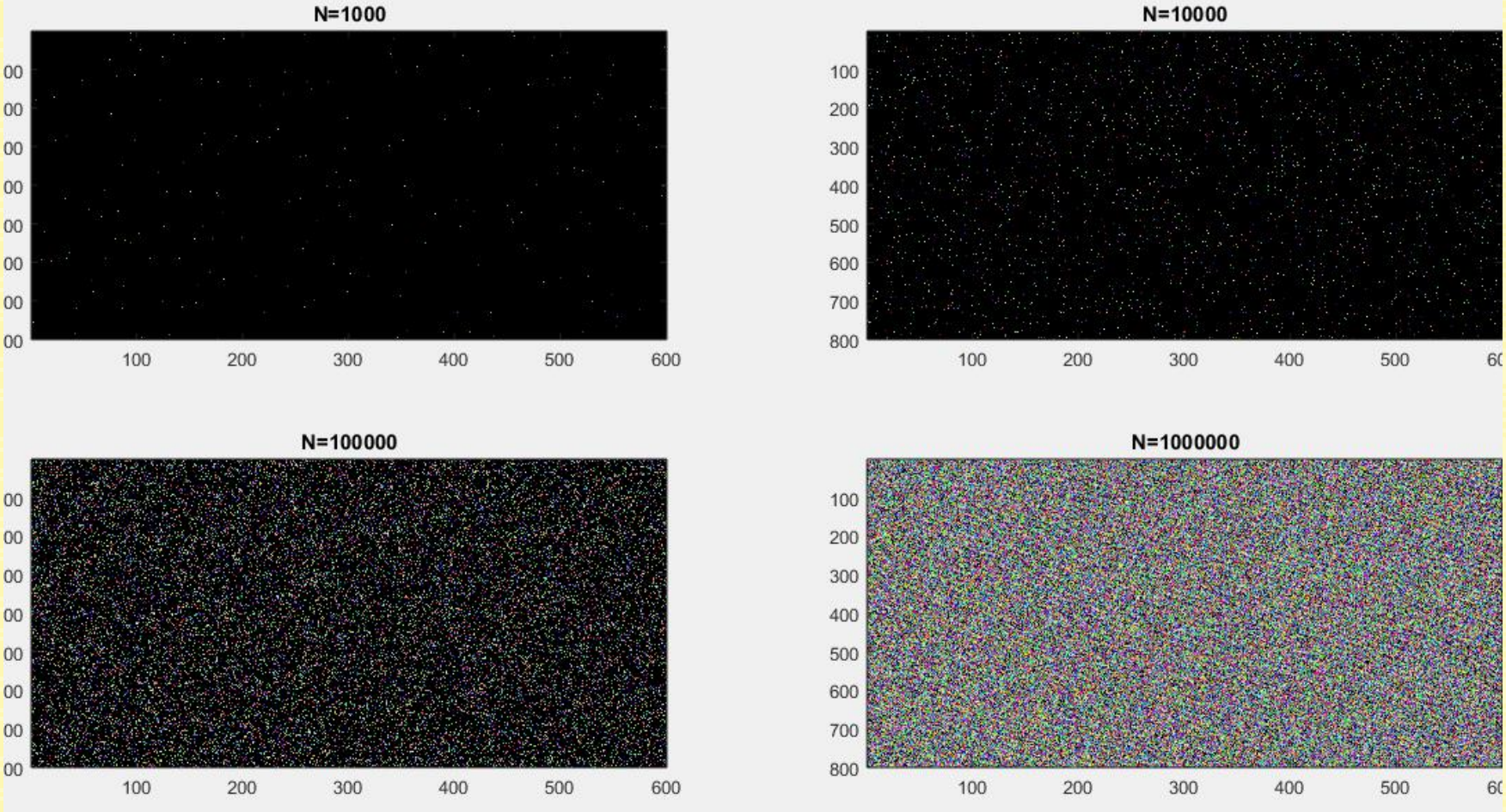
ГРАФИЧЕСКИЙ ТЕСТ



Линейный конгруэнтный генератор a=100, c=1, X_0=6421, m=23211121111

РЕЗУЛЬТАТЫ ПРОВЕРОК

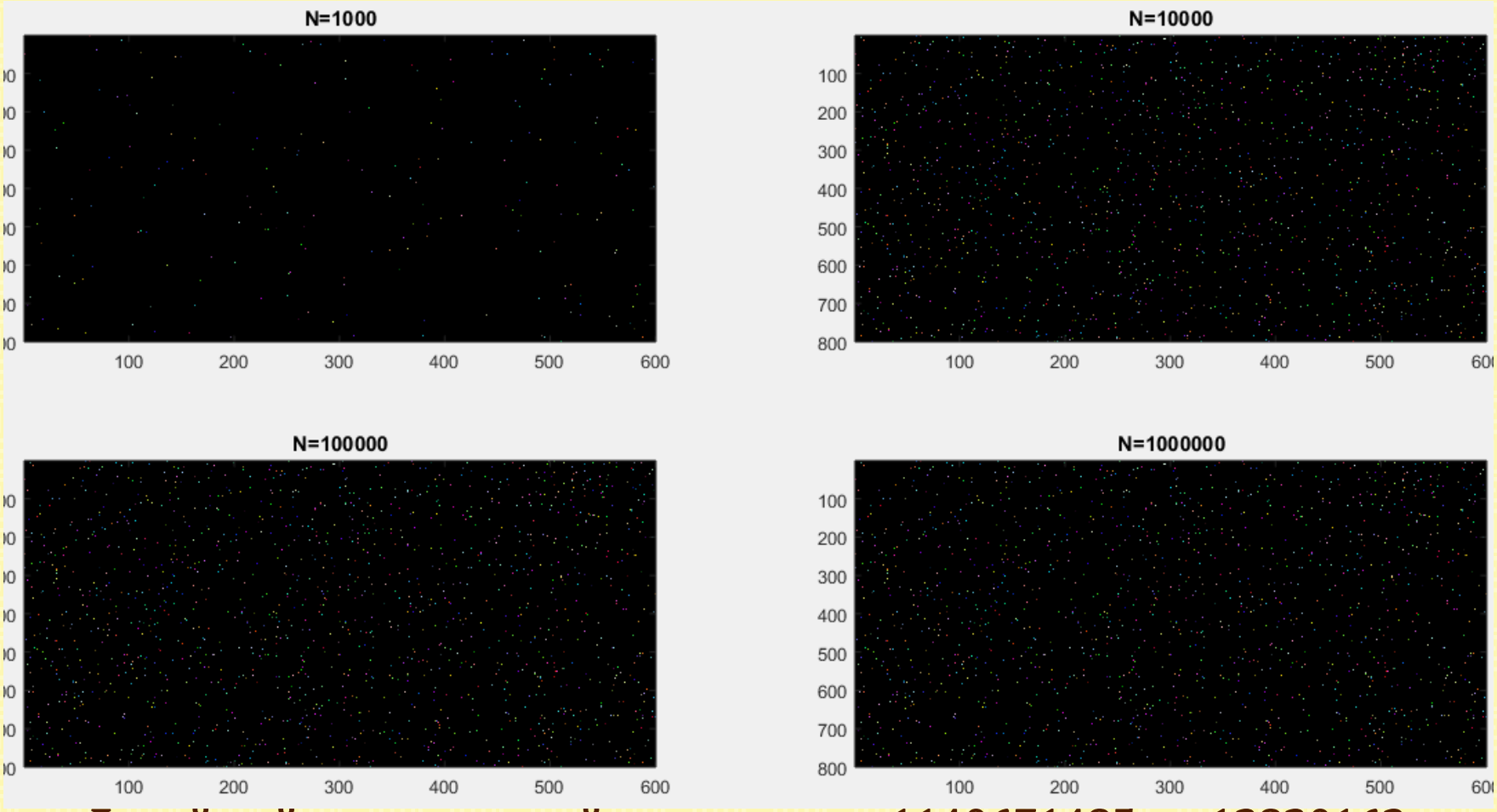
ГРАФИЧЕСКИЙ ТЕСТ



Линейный конгруэнтный генератор a=2416, b=374441, m=1771875, X_0=6421

РЕЗУЛЬТАТЫ ПРОВЕРОК

ГРАФИЧЕСКИЙ ТЕСТ



Линейный конгруэнтный генератор a=1140671485, c=12820163, m=16777216, X_0=327680

ВЫЧИСЛЕНИЕ ЧИСЛА π МЕТОДОМ МОНТЕ-КАРЛО

По результатам проверок были выбраны генераторы:

1. Линейный конгруэнтный генератор с параметрами $a=2416$, $b=374441$, $m=1771875$, $X_0=6421$
2. Генератор BBS с параметрами $p=999983$, $q=999979$, $X=6421$
3. Генератор Фибоначчи с лагами $a=97$, $b=33$

ВЫЧИСЛЕНИЕ ЧИСЛА π МЕТОДОМ МОНТЕ-КАРЛО

$$\pi \approx \frac{4N_{\text{кр}}}{N_{\text{кв}}}$$

$N_{\text{кр}}$ – число точек, попавших в круг, вписанный в квадрат;

$N_{\text{кв}} = N$ – число точек, вброшенных в квадрат.

Точки формируются из элементов ПСП - (X_i, X_{i+1}).

ВЫЧИСЛЕНИЕ ЧИСЛА π МЕТОДОМ МОНТЕ-КАРЛО

Приближенные значения числа π

	$N = 10^5$	$N = 10^6$	$N = 10^7$
Линейный конгруэнтный генератор, m =1771875, a=2416, c=374441	3.14184167	3.14154137	3.14153334
BBS, p=999983, q=999979	3.14546582	3.14015776	3.14122190
Генератор Фибоначчи, a=97, b=33	3.14398976	3.14062616	3.14178066

ВЫЧИСЛЕНИЕ ЧИСЛА π МЕТОДОМ МОНТЕ-КАРЛО

Лучшим можно считать генератор, для которого минимальным является значение:

$$\left|\left[\frac{\pi N}{4}\right] - N_{\text{кр}}\right|$$

	$N = 10^5$	$N = 10^6$	$N = 10^7$
Линейный конгруэнтный генератор, m =1771875, a=2416, c=374441	100	106	153
BBS, p=999983, q=999979	156	490	928
Генератор Фибоначчи, a=97, b=33	174	473	1640

ВЫЧИСЛЕНИЕ ЧИСЛА π МЕТОДОМ МОНТЕ-КАРЛО

Наилучшим генератором для решения данной задачи методом статистических испытаний оказался **линейный конгруэнтный генератор** с параметрами m=1771875, a=2416, c=374441. Но для более точных результатов он не подойдет, т. к. слишком маленький период ($T=m$=1771875).

ВЫВОДЫ

На сегодняшний день существует достаточно много алгоритмов и генераторов для формирования ПСП, в данной работе были рассмотрены лишь наиболее популярные. И те проверки, что были использованы, не могут однозначно ответить на вопрос, какой генератор на самом деле лучший, однако эти проверки являются основными и способны выявить явные недостатки тех или иных генераторов, что, собственно, и отражено в результатах.

Спасибо за внимание!