Завгородний Станислав Дмитриевич

студент

ФГАОУ ВО «Самарский национальный исследовательский университет им. академика С.П. Королева»

г. Самара, Самарская область

КОНГРУЭНТНЫЕ ГЕНЕРАТОРЫ

Аннотация: *в статье рассматриваются общие принципы работы конгруэнтных генераторов. В основе работы лежат понятия о псевдослучайных числах и числовых последовательностях. Автором реализуется квадратичный конгруэнтный генератор.*

Ключевые слова: *псевдослучайные числа, числовая последовательность.*

Основные понятия

Введем некоторые определения, которые будут использованы в работе.

Определение 1. Псевдослучайные числа – числа генерируемой последовательности, элементы которой подчиняются заданному закону распределения и почти не зависят друг от друга.

Определение 2. Числовая последовательность – последовательность элементов числового пространства.

Введение

Программистам в своей работе очень часто приходится сталкиваться с необходимостью работы со случайными числами. Обычно такие числа применяются в задачах моделирования, тестирования программ, численного анализа, а также во множестве специфических задач. Во многих современных языках программирования для таких нужд предусмотрена функция random или ее альтернативы. Зачастую они выдают хорошие псевдослучайные числа. В основном в этой функции применяется работа конгруэнтных генераторов.

Линейные конгруэнтные генераторы

Программный генератор, который порождает с помощью рекуррентного соотношения $x_{t+1} = (ax_t + c) \bmod N$ $(t = 0, 1,..)$ псевдослучайную последовательность

x1, x2,... принадлежащую A, где A = {0, 1,..., N-1} называется линейным конгруэнтным генератором с параметрами (x_0, a, c, N). Параметры такого генератора имеют следующий смысл: x_0 принадлежит A и является стартовым значением, параметр *a* также принадлежит A и является ненулевым множителем, *c* – приращение, тоже принадлежит A, *N* – модуль, равный мощности алфавита A. В случае если приращение *c=0*, генератор называется мультипликативным конгруэнтным генератором. В противоположном случае генератор называется смешанным конгруэнтным генератором.

Квадратичные конгруэнтные генераторы

Алгоритм, который генерирует псевдослучайные числа x_t, принадлежащие A = {0, 1,.. N-1}, с помощью квадратичного рекуррентного соотношения $x_{t+1} = (dx_t^2+ax_t + c) \bmod N$ (t = 0, 1,..) называется квадратичным конгруэнтным генератором с параметрами (x_0, a, c, d, N). В таких генераторах отсутствует слабость, присущая линейным конгруэнтным генераторам, которая может применятся для проведения криптоатак в целях оценки параметров a, c, x_0. Если параметры a = d = 1 и c = 0 генератор называется генератором Ковью.

Реализация квадратичного конгруэнтного генератора

Программа генерирования псевдослучайных чисел с помощью квадратичного конгруэнтного генератора была реализована языке программирования C++. Программа также высчитывает период повторения генерируемых чисел. Код программы:

```
#pragma hdrstop
#include <stdio.h>
#include <stdlib.h>
#include <time.h>
int A,C,D,X,i,X2,p1,p2, M, N;
randomize();
cout << «Vvedite koefficient A!\n»; cin >> A;
cout << «Vvedite koefficient D!\n»; cin >> D;
cout << «Vvedite koefficient C!\n»; cin >> C;
```

```
cout << «Vvedite nachalnoe znachenie X0!\n»; cin >> X;
cout << «Vvedite module!\n»; cin >> M;
cout << «Vvedite kolichestvo generiruemah chisel N!\n»; cin >> N;
for (i = 2; i < N; i++) {
X2=(D*(int(pow(X,2)))+(A*X)+C) % M;
if (i== (N % 4)) { p1=X2; }
if ((i>(N % 4))&&(X2==p1)) {p2=i-(N % 4); p1=111111;}
X=X2;
cout << i << " = " << X2 << "\n»;
}
cout << «Период = " << p2 << "\n»;
}
```

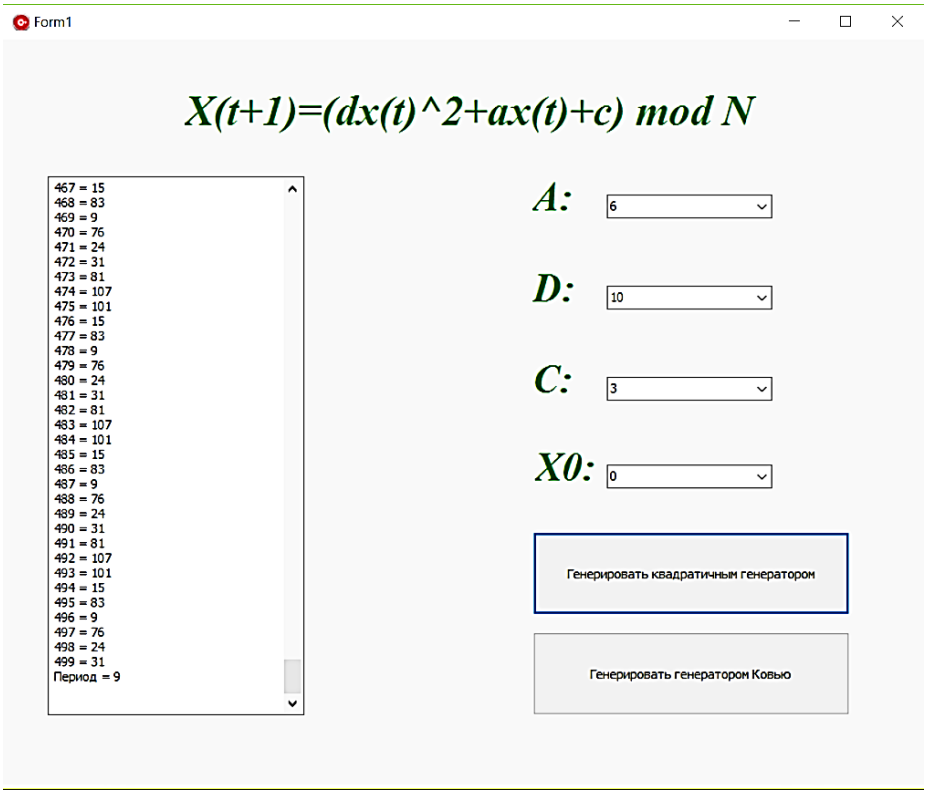

Рис. 1. Пример реализованного квадратичного конгруэнтного генератора с адаптацией кода программы под среду разработки C++ Builder

Список литературы

1. Кнут Д.Э. Глава 3. Случайные числа // Искусство программирования (The Art of Computer Programming). Т. 2. Получисленные алгоритмы. – 3-е изд. – М.: Вильямс, 2000. – 832 с.