МИНОБРНАУКИ РОССИИ
ФГБОУ ВО «СГУ ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»

ЛАБОРАТОРНАЯ РАБОТА №4

студента 4 курса 431 группы
направления 10.05.01 — Компьютерная безопасность
факультета КНиИТ
Никитина Арсения Владимировича

Проверил
доцент ______________ А. В. Жаркова

Саратов 2022

СОДЕРЖАНИЕ

1 Задание лабораторной работы

Пусть задан мультипликативный конгруэнтный генератор:

$$x_{t+1} = \alpha x_t (mod\, n)$$

Предположим, что НОД($x_0,\ n$) = 1. Каково возможное максимальное значение периода выпускной последовательности?

2 Теоретическая часть

2.1 Лемма о разложении числа на простые множители

Пусть число n допускает разложение на простые множители в виде:

$$n = p_1^{e_1} \times p_2^{e_2} ... \times p_k^{e_k}$$

.

Длина периода мультипликативной конгруэнтной последовательности, определенной параметрами (x_0, α, m), является наименьшим общим кратным длин периодов последовательностей ($x_0 \, mod \, p_j^{e_j}, \; \alpha_0 \, mod \, p_j^{e_j}, \; p_j^{e_j}$).

Для начала рассмотрим любое число n. Оно может быть как простым так и нет.

2.2 Случай 1. Число n не является простым

Рассмотрим ситуацию, когда n — составное число. Итак, если число n имеет делитель d, и если x_t , будет кратно этому числу d, то все последующие элементы последовательности начиная с x_{t+1}, то есть последовательность будет вырождаться в 0 начиная с этого числа. Так что нам необходимо, чтобы не только начальный элемент последовательности (x_0) был взаимнопрост с n, но и все последующие, что и будет ограничивать период последовательности до значения функции Эйлера от числа n, то есть до количества взаимнопростых с числом n чисел в промежутке от 1 до $n - 1$.

Согласно приведенной лемме период последовательности зависит исключительно от периодов последовательностей при $n = p^e$

Итак, если $x_t = \alpha^t x_0 \; mod \; p^e$ и ясно, что период будет иметь длину 1, если α будет кратно p. Поэтому будем считать, что a и p взаимнопростые. Тогда период будет наименьшим целым числом λ, таким, что $x_0 = \alpha^\lambda x_0 \, mod \, p^e$. Если НОД($x_0, p^e$) = p^f, то это можно переписать как:

$$\alpha^\lambda \equiv 1 (mod \, p^{e-f})$$

. Поэтому λ является делителем $\varphi(p^{e-f}) = p^{e-f-1}(p-1)$.

Когда α и m — взаимнопростые числа, наименьшее число λ, для которого $\alpha^\lambda \equiv 1 \; (mod \; n)$, принято называть порядком α по модулю n. Любое такое значение α, которое имеет максимальный возможный порядок по модулю m, называется первообразным элементом по модулю m.

Обозначим через $\lambda(n)$ порядок первообразного элемента. Так как $p^{e-1}(p-1) \vdots \lambda(p^e)$, то можно определить и порядок m с помощью следующих соотношений:

$$\lambda(2) = 1,$$
$$\lambda(4) = 2,$$
$$\lambda(2^e) = 2^{e-2}, \text{ если } e \geq 3,$$
$$\lambda(p^e) = p^{e-1}(p-1), \text{ если } e > 2,$$
$$\lambda(p_1^{e_1} \times p_2^{e_2} ... \times p_k^{e_k}) = \text{НОК}(\lambda(p_1^{e_1}), ..., \lambda(p_k^{e_k})), \text{ если } e > 2.$$

2.3 Случай 2. Число n простое

Так как мы выяснили, что длина периода ограничена значением функции Эйлера, то можем получить, что для простого числа значение функции Эйлера максимально и равно количеству взаимно простых с ним, то есть $n-1$.

2.4 Объединение случаев

Так как по условию имеем x_0 и n — взаимнопросты, то длина периода будет зависеть от степени перовобразного элемента в общем случае и не будет зависеть от этого, когда само число n является простым и максимальный период для данного числа известен и равен $n-1$.