Отчёт по лабораторной работе №6

Дисциплина: Математические основы защиты информации и информационной безопасности

Полиенко Анастасия Николаевна, НПМмд-02-23

Содержание

# 1 Цель работы

Изучить алгоритмы разложения числа на множители.

# 2 Задание

Реализовать алгоритм p-метода Полларда.

# 3 Теоретическое введение

Задача разложения на множители - одна из первых задач, использованных для построения криптосистем с открытым ключом.

*Задача разложения составного числа на множители* формулируется следующим образом: для данного положительного целого числа найти его каноническое разложение , где - попарно различные простые числа,

На практике не обязательно находить каноническое разложение числа . Достаточно найти его разложение на два *нетривиальных сомножителя:* . Далее будем понимать задачу разложения именно в этом смысле.

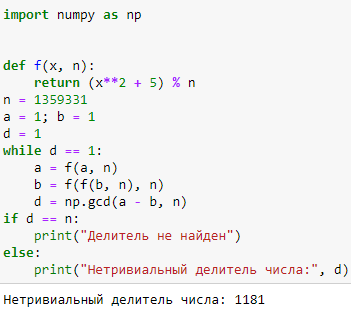
*p-Метод Полларда.* Пусть - нечетное составное число, и - случайное отображение, обладающее сжимающими свойствами, например . Основная идея метода состоит в следующем. Выбираем случайный элемент и строим последовательность , определяемую рекуррентным соотношением

где , до тех пор, пока не найдем такие числа , что и . Поскольку множество конечно, такие индексы существуют (последовательность «зацикливается»). Последовательность будет состоять из «хвоста» длины той же длины.

Более подробно см. в [1–6].

# 4 Выполнение лабораторной работы

Реализуем алгоритм алгоритм p-метода Полларда. (рис. ??)



p-метод Полларда.

# 5 Выводы

Изучила алгоритмы разложения числа на множители.

# Список литературы

1. GNU Bash Manual [Электронный ресурс]. Free Software Foundation, 2016. URL: <https://www.gnu.org/software/bash/manual/>.

2. Newham C. [Learning the bash Shell: Unix Shell Programming](http://www.amazon.com/Learning-bash-Shell-Programming-Nutshell/dp/0596009658). O’Reilly Media, 2005. 354 с.

3. Zarrelli G. Mastering Bash. Packt Publishing, 2017. 502 с.

4. Robbins A. [Bash Pocket Reference](https://www.ncbi.nlm.nih.gov/pubmed/25246403). O’Reilly Media, 2016. 156 с.

5. Таненбаум Э. Архитектура компьютера. 6-е изд. СПб.: Питер, 2013. 874 с.

6. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.