Отчет по лабораторной работе №6

Разложение чисел на множители

Бармина Ольга Константиновна

2024 September 7th

Содержание

# 1 Цель работы

Целью данной работы является освоение *p-метода Полларда*, который является одним из алгоритмом разложения составного числа на множители.

# 2 Задание

1. Изучить алгоритм разложения чисел на множители.
2. Реализовать представленный алгоритм и разложить на множители заданное число.

# 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 *n* найти его каноническое разложение , где - попарно различные простые числа, .

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

*p-Метод Полларда*. Пусть *n* - 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

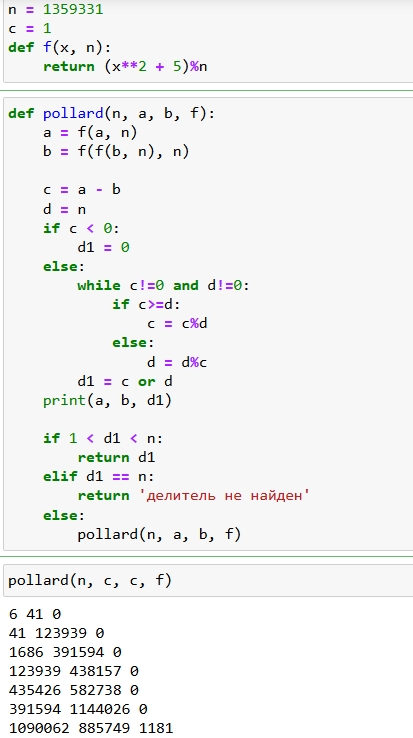
где , до тех пор, пока не найдем такие числа , что и . Поскольку множество конечно, такие индексы существуют (последовательность “зацикливается”) [[2]](https://esystem.rudn.ru/pluginfile.php/2089897/mod_folder/content/0/mathsec_lection12-message-integrity-authentication.pdf?forcedownload=1). Последовательность будет состоять из “хваста” длины и цикла той же длины.

# 4 Выполнение лабораторной работы

Для реализации рассмотренного алгоритма разложения чисел на множители используется среда Google Colab.

1. Запишем алгоритм, реализующий *р-метод Полларда*. Проверим корректность работы алгоритма для заданных сведений. Для этого запишем условие примера с помощью следующей функции:

При вызове данной функции видим, что получаем то же число, что было описано в примере. То есть является нетривиальным делителем числа .



Реализация метода Полларда

# 5 Выводы

В ходе работы мы изучили и реализовали вероятностные алгоритмы проверки чисел на простоту.

# 6 Список литературы

1. Фороузан Б. А. Криптография и безопасность сетей. - М.: Интернет-Университет Информационных Технологий : БИНОМ. Лаборатория знаний, 2010. - 784 с. [[1]](https://intuit.ru/studies/courses/552/408/lecture/9350)
2. Методические материалы курса [[2]](https://esystem.rudn.ru/pluginfile.php/2089897/mod_folder/content/0/mathsec_lection12-message-integrity-authentication.pdf?forcedownload=1)