Отчёт по лабораторной работе №6. Разложение чисел на множители

Дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Майорова О.А., 1032212322
Группа: НФИмд-02-21
Преподаватель: д.ф.-м.н., Кулябов Д. С.

Москва, 2021

Цель и задачи

Цель: Ознакомиться с задачей разложения составного числа на множители.

Задача: Программно реализовать ρ-метод Полларда.

Теоретическое введение

Факторизация — разложение натурального числа в произведение простых множителей.

Основная теорема арифметики: $n = p_1^{e1} \times p_2^{e_2} \times \cdots \times p_k^{e_k}$, где $p_1, p_2, \ldots, p_k$ — простые числа и $e_1, e_2, \ldots, e_k$ — положительные целые числа.

ρ-метод Полларда

Вход: Число n, начально значение c, функция f, обладающая сжимающими свойствами.

1. Положить $a \leftarrow c, b \leftarrow c$
2. Вычислить $a \leftarrow f(a)(\mod n), b \leftarrow f(f(b))(\mod n)$
3. Найти $d \leftarrow \text{НОД}(a - b, n)$
4. Если $1 < d < n$, то результат d. При $d = n$ результат “Делитель не найден”. При $d = 1$ вернуться на шаг 2.

Реализация ρ-метода Полларда

Положительное целое число $n = 1359331$

Начальное значение $c = 1$

Функция, обладающая сжимающими свойствами:
$f(x) = (x^2 + 5) \mod n$

Проверка функции ρ-метода Полларда:

```
1 Pollard(1, 1359331)
```

```
1181
```

Заключение

Таким образом, была достигнута цель, поставленная в начале лабораторной работы.

- Было осуществлено знакомство с задачей разложения составного числа на два нетривиальных сомножителя.
- Также была получена реализация на языке Python ρ-метода Полларда.

Спасибо за внимание