Лабораторная работа 6

Попов Дмитрий Павлович, НФИмд-01-23

Содержание

List of Figures

List of Tables

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра математического моделирования и искусственного интеллекта

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6

дисциплина: Математические основы защиты информации и информационной безопасности

Преподователь: Кулябов Дмитрий Сергеевич

Студент: Попов Дмитрий Павлович

Группа: НФИмд-01-23

МОСКВА

2023 г.

1 Цель работы

Освоить на практике разложение чисел на множители.[1]

2 Выполнение лабораторной работы

Требуется реализовать:

1. Алгоритм, реализующий p-метод Полларда

2.1 p-метод Полларда

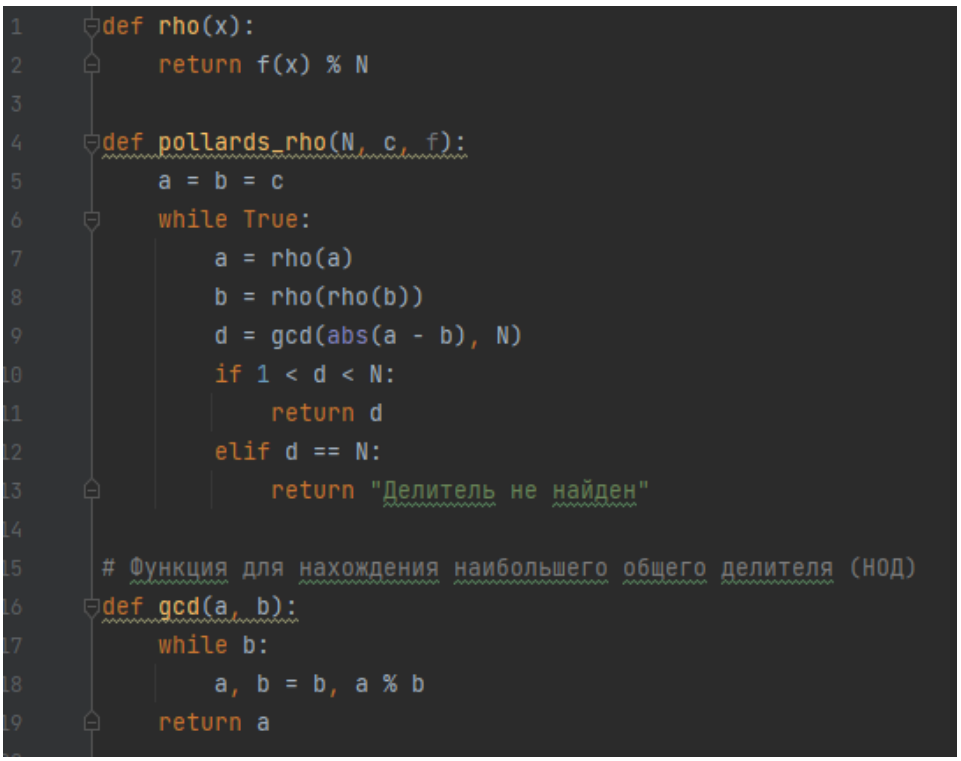
Метод Полларда применяется при факторизации натуральных чисел.

Основные шаги:

Вход: число N, начальное значение c, функция f, обладающая сжимающими свойствами Выход: нетривиальный делительно числа n 1) положить a <- c, b <- c 2) Вычислить a Б- f(a)(mod n), b <- f(b) (mod n) 3) Найти d <- НОД(a-b, n) 4) Если 1< d< n, То положить p <- dи результат: p. При d=n результат: “Делитель не найден”; при d=1 вернуться на шаг 2

Чтобы реализовать программу был написал след. код на python:

1. Функция, реализующая p-метод Полларда
2. Функция нахождения НОД fig. 2.1.



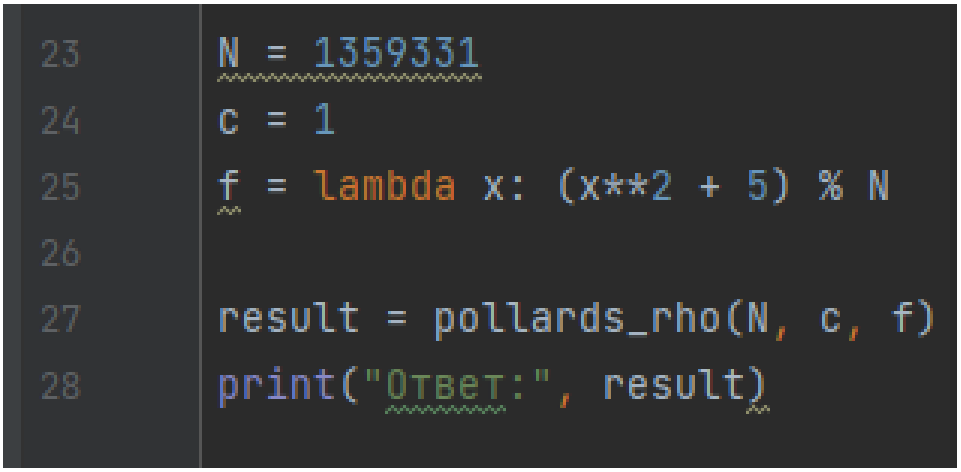
```
def rho(x):
    return f(x) % N

def pollards_rho(N, c, f):
    a = b = c
    while True:
        a = rho(a)
        b = rho(rho(b))
        d = gcd(abs(a - b), N)
        if 1 < d < N:
            return d
        elif d == N:
            return "Делитель не найден"

# Функция для нахождения наибольшего общего делителя (НОД)
def gcd(a, b):
    while b:
        a, b = b, a % b
    return a
```

Figure 2.1: pollard

Начальные данные для запуска функции fig. 2.2.



```
N = 1359331
c = 1
f = lambda x: (x**2 + 5) % N

result = pollards_rho(N, c, f)
print("Ответ:", result)
```

Figure 2.2: init

Выходные значения программы (пример из методички) fig. 2.3.

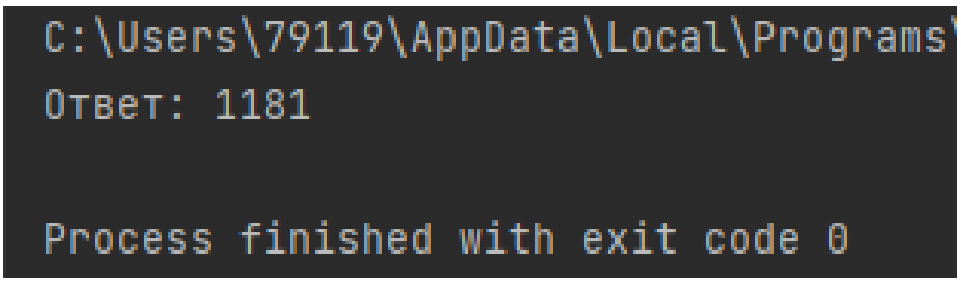


Figure 2.3: output

3 Выводы

В результате выполнения работы я освоил на практике алгоритм разложения чисел на множители.

4 Список литературы

1. Методические материалы курса