Математические основы защиты информации и информационной безопасности. Лабораторная работа №6

Разложение чисел на множители

Содержание

# 1 Цель работы

Изучение алгоритма разложения составного числа на множители.

# 2 Задачи

Реализовать программно алгоритм, реализующий p-метод Полларда

# 3 Теоретические сведения

Любое натуральное число n > 1 можно представить в виде произведения простых чисел. Это представление называется разложением числа n на простые множители. [1]

p-алгоритм Полларда строит числовую последовательность, элементы которой образуют цикл, начиная с некоторого номера n, что может быть проиллюстрировано, расположением чисел в виде греческой буквы p, что послужило названием семейству алгоритмов.Иллюстрацию этого алгоритма на плоскости можно увидеть на рис. 1

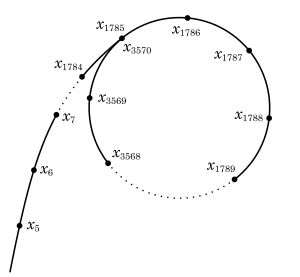


Figure 1: Зацикливание числовой последовательности

## 3.1 p-метод Полларда

* Вход. Число , начальное значение , функция , обладающая сжимающими свойствами.
* Выход. Нетривиальный делитель числа .

1. Положить
2. Вычислить
3. Найти
4. Если 1 < < , то положить и результат: . При результат: “Делитель не найден”; при вернуться на шаг 2.

Подробнее об алгоритме: [2]

# 4 Выполнение работы

## 4.1 Реализация алгоритмов

def euclid(a, b):  
 r = []  
 r.append(a)  
 r.append(b)  
 i = 1  
 while True:  
 r.append(r[i - 1] % r[i])  
 if r[i + 1] == 0:  
 d = r[i]  
 return d  
 else:  
 i = i + 1  
  
  
def pollard(n, c):  
 a = c  
 b = c  
 while True:  
 a = f(a, n) % n  
 b = f(f(b, n), n) % n  
 first = min(a - b, n)  
 second = max(a - b, n)  
 d = euclid(first, second)  
 if d > 1 and d < n:  
 p = d  
 return p  
 elif d == n:  
 return -1  
 elif d == 1:  
 continue  
  
  
def f(x, n):  
 return (x \*\* 2) + 5 % n  
  
  
if \_\_name\_\_ == '\_\_main\_\_':  
 n = int(input("Введите число n: "))  
 c = int(input("Введите число c: "))  
 result = pollard(n, c)  
 print("Нетривиальный делитель числа n = {}".format(result))

## 4.2 Пример работы алгоритма Ферма

На рис. 2 представлены результаты работы p-метода Полларда:

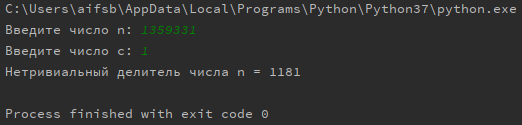


Figure 2: Пример работы алгоритма Ферма

# 5 Выводы

В ходе выполнения работы был успешно изучен p-метод Полларда, а также был реализован программно программно на языке Python.

# Список литературы

1. Разложение числа на множители онлайн [Электронный ресурс]. umath, 2021. URL: <https://umath.ru/calc/factorization/>.

2. Алгоритм Ферма [Электронный ресурс]. Википедия, 2021. URL: <https://ru.wikipedia.org/wiki/Ро-алгоритм_Полларда>.