

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ
Факультет физико-математических и естественных наук
Кафедра прикладной информатики и теории вероятностей

Отчёт по лабораторной работе №6. Разложение чисел на множители

*Дисциплина: Математические основы защиты
информации и информационной безопасности*

Студент: Лапшенкова Любовь Олеговна, 10322127633

Группа: НФИмд-02-21

Преподаватель: Кулябов Дмитрий Сергеевич,
д-р.ф.-м.н., проф.

Москва 2021

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
3.1	Р-алгоритм Полларда	7
3.2	(Р-1) алгоритм Полларда	8
4	Выполнение лабораторной работы	9
4.1	Р-метод Полларда	9
5	Выводы	13
	Список литературы	14

List of Figures

4.1	Входные данные для реализации алгоритма для разложения чисел на множители	9
4.2	Реализация алгоритма р-метод Полларда	10
4.3	Реализация алгоритма р-метод Полларда	11
4.4	Результат реализации алгоритма р-метод Полларда на примере .	12

List of Tables

1 Цель работы

Целью данной лабораторной работы является ознакомление с алгоритмами для разложения чисел на множители.

2 Задание

1. Реализовать рассмотренный в инструкции к лабораторной работе алгоритм для разложения чисел на множители программно.
2. Разложить на множители данное в примере к лабораторной работе число.

3 Теоретическое введение

В данной лабораторной работе предметом нашего изучения стал Р-метод Полларда. ## Факторизация целых чисел

Факторизацией натурального числа называется его разложение в произведение простых множителей. Существование и единственность (с точностью до порядка следования множителей) такого разложения следует из основной теоремы арифметики.

В отличие от задачи распознавания простоты числа, факторизация предположительно является вычислительно сложной задачей. В настоящее время неизвестно, существует ли эффективный не квантовый алгоритм факторизации целых чисел. Однако доказательства того, что не существует решения этой задачи за полиномиальное время, также нет.

Предположение о том, что для больших чисел задача факторизации является вычислительно сложной, лежит в основе широко используемых алгоритмов (например, RSA). Многие области математики и информатики находят применение в решении этой задачи [1].

3.1 Р-алгоритм Полларда

Р-алгоритм (ρ -алгоритм) — предложенный Джоном Поллардом в 1975 году алгоритм, служащий для факторизации (разложения на множители) целых чисел. Данный алгоритм основывается на алгоритме Флойда поиска длины цикла в последовательности и некоторых следствиях из парадокса дней рождения. Ал-

горитм наиболее эффективен при факторизации составных чисел с достаточно малыми множителями в разложении [2].

Также хотелось бы упомянуть P-1 алгоритм Полларда.

3.2 (P-1) алгоритм Полларда

(P-1) алгоритм Полларда впервые опубликован британским математиком Джоном Поллардом в 1974 году. Именно появление данного алгоритма привело к изменению понятия сильного простого числа, используемого в криптографии, нестрого говоря, простого числа, для которого $p-1$ имеет достаточно большие делители. В современных криптосистемах стараются использовать именно сильные простые числа, так как это повышает стойкость используемых алгоритмов и систем в целом [3].

4 Выполнение лабораторной работы

Примечание: комментарии по коду представлены на скриншотах к каждому из проделанных заданий.

В соответствии с заданием, была написана программа по воплощению алгоритма по разложению чисел на множители.

Программный код и результаты выполнения программ представлен ниже.

4.1 Р-метод Полларда

```
n=1359331#ввели число n
с=1#ввели начальное значение с
```

Figure 4.1: Входные данные для реализации алгоритма для разложения чисел на множители

```

def f(x,n):
    '''
    ввод функции, обладающей сжимающими свойствами
    '''
    return (x**2+5)%n

def algorithm_Evklida(a,b):
    '''
    Расписываем пункты 1-4 для алгоритма Евклида
    '''
    r=[]
    r.append(a)
    r.append(b)
    i=1
    while r[i]!=0:
        i+=1
        r.append(r[i-2]%r[i-1])
    d=r[i-1]
    return d

```

Figure 4.2: Реализация алгоритма р-метод Полларда

```

def method_Pollarda(n,c):
    #пункт 1
    a=c
    b=c
    while True:
        #пункт 2
        a=f(a,n)%n
        b=f(f(b,n),n)%n
        #пункт 3
        d=algorithm_Evklida(a-b,n)
        #пункт 4
        if 1<d<n:
            p=d
            return p
        if d==n:
            return 'Делитель не найден'
method_Pollarda(n,c)

```

Figure 4.3: Реализация алгоритма р-метод Полларда

Были взяты данные из пояснения к лабораторной работе. Они были подставлены в программу. Получен следующий результат (см. рис. [-fig. ??]).

1181

Figure 4.4: Результат реализации алгоритма р-метод Полларда на примере

5 Выводы

Таким образом, была достигнута цель, поставленная в начале лабораторной работы: я ознакомилась с алгоритмом разложения чисел (Р-методом Полларда), реализовала данный алгоритм на языке программирования Python 3, получила результат, схожий с данным в описании к лабораторной работе.

Список литературы

1. Википедия. Факторизация целых чисел [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%BA%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F_%D1%86%D0%B5%D0%BB%D1%8B%D1%85_%D1%87%D0%B8%D1%81%D0%B5%D0%BB (дата обращения: 16.12.2021).
2. Википедия. Ро-алгоритм Полларда [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: https://ru.wikipedia.org/wiki/%D0%A0%D0%BE-%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%9F%D0%BE%D0%BB%D0%BB%D0%B0%D1%80%D0%B4%D0%B0 (дата обращения: 16.12.2021).
3. Википедия. Р-1-алгоритм Полларда [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: https://ru.wikipedia.org/wiki/P%E2%88%921-%D0%BC%D0%B5%D1%82%D0%BE%D0%B4_%D0%9F%D0%BE%D0%BB%D0%BB%D0%B0%D1%80%D0%B4%D0%B0 (дата обращения: 16.12.2021).