МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КУБГУ»)**

**Факультет компьютерных технологий и прикладной математики**

**Кафедра вычислительных технологий**

**Отчет**

**по практическому заданию №1**

**по курсу**

**«КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ»**

Работу выполнил

Студенты 46 группы

Нагалевский А.М.

Преподаватель:

Крамаренко А.А.

Краснодар 2024

**Постановка задачи.**

Реализовать программный продукт нахождения функции Эйлера от числа двумя способами (по определению и с помощью формулы). Сравнить эффективность алгоритмов для набора из 100 чисел, каждое из которых больше 10’000’000.

Функция Эйлера является важным понятием в теории чисел. Она называется в честь математика Леонарда Эйлера, который внес значительный вклад в различные области математики, включая теорию чисел.

Функция Эйлера определяется как количество положительных целых чисел, меньших или равных n, и взаимно простых с n. Взаимная простота двух чисел означает, что их наибольший общий делитель (НОД) равен 1.

Например, = 4, потому что среди чисел 1, 2, 3, 4, 5, 6, 7, 8 только 1, 3, 5, 7 взаимно просты с 8.

Важно отметить несколько ключевых свойств функции Эйлера:

1. Если n - простое число, то . Это следует из того, что все числа, меньшие простого числа n, будут взаимно просты с ним.
2. Для любых двух взаимно простых чисел a и b верно: . Это свойство называется мультипликативностью функции Эйлера.
3. Если p - простое число, а k - натуральное число, то . Это следует из свойства мультипликативности и того, что взаимно простыми с являются все числа, кроме кратных p.

Рассмотрим два способа вычисления функции Эйлера: по определению и с использованием формулы для простых чисел.

1. Вычисление по определению:

Этот способ основывается на определении функции Эйлера, где - количество положительных целых чисел, меньших или равных n, и взаимно простых с n.

Алгоритм по определению состоит из следующих шагов:

1. Начинаем с 1 и перебираем все числа до n.
2. Для каждого числа проверяем, является ли оно взаимно простым с n, то есть имеет ли оно НОД равный 1.
3. Если НОД равен 1, увеличиваем счетчик на 1.
4. По завершении перебора, возвращаем значение счетчика как результат.

Этот метод прост в реализации, но его эффективность снижается с увеличением значения n, так как требует проверки НОД для каждого числа.

1. Вычисление с использованием формулы для простых чисел:

Для простых чисел p, существует простая формула: = p - 1.

Более общая формула основана на свойствах функции Эйлера и простых чисел. Пусть - различные простые числа. Тогда функция Эйлера для n выражается как:

Эта формула позволяет быстро вычислить значение функции Эйлера для любого числа, представленного в виде произведения простых чисел.

Теперь сравним эти два метода:

* Вычисление по определению просто в реализации, но требует больше времени на выполнение, особенно для больших значений n. В моей реализации на языке Python для набора из 100 случайных чисел, каждое из которых больше 10’000’000 время получилось следующее: 1265.5 секунд или 21 минут, что очень долго.
* Вычисление с использованием формулы для простых чисел более эффективно и быстро работает даже для больших значений n, но требует знания простых множителей числа n. В моей реализации на языке Python для набора из 100 случайных чисел, каждое из которых больше 10’000’000 время получилось следующее: 0.02 секунды, что очень быстро, особенно сравнивая с первым методом.

**Текст программы:**

**Файл LR1.py:**

from math import gcd

import time

import random

def euler\_definition(n):

count = 0

for i in range(1, n + 1):

if gcd(n, i) == 1:

count += 1

return count

def euler\_formula(n):

result = n

p = 2

while p \* p <= n:

if n % p == 0:

while n % p == 0:

n //= p

result -= result // p

p += 1

if n > 1:

result -= result // n

return result

number = 15

print("Функция Эйлера по определению для", number, ":", euler\_definition(number))

print("Функция Эйлера с использованием формулы для", number, ":", euler\_formula(number))

random\_numbers = [random.randint(10\_000\_001, 100\_000\_000) for \_ in range(100)]

start\_time = time.time()

for num in random\_numbers:

euler\_definition(num)

end\_time = time.time()

definition\_time = end\_time - start\_time

start\_time = time.time()

for num in random\_numbers:

euler\_formula(num)

end\_time = time.time()

formula\_time = end\_time - start\_time

print("Время выполнения для функции Эйлера по определению:", definition\_time)

print("Время выполнения для функции Эйлера с использованием формулы:", formula\_time)