Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**«Отчёт по лабораторной работе №1»**

“ОСНОВЫ ТЕОРИИ ЧИСЕЛ И ИХ ИСПОЛЬЗОВАНИЕ В КРИПТОГРАФИИ”

**Выполнил:** студент 3 курса

3 группы специальности ИСИТ

Шедько Евгений Александрович

**Проверил:** преподаватель

Копыток Дарья Владимировна

Минск 2022

**Вариант 14**

**1. Используя L\_PROST, найти все простые числа в интервале [2, n]. Значение n соответствует варианту из табл. 1.2, указанному преподавателем.**

В соответствии с вариантом n = 663. Результат работы программы представлен на Рис. 1.

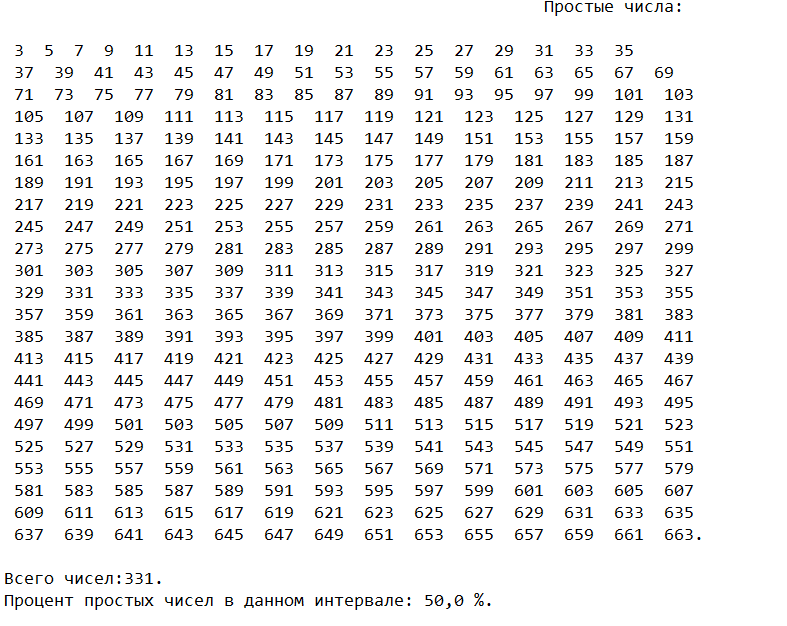


Рис.1 Результат нахождения простых чисел в программе L\_PROST

n/ln(n) = 102.05063

**2. Повторить п. 1 для интервала [m, n]. Сравнить полученные результаты с «ручными» вычислениями, используя «решето Эратосфена» (см. примеры 11 и 12).**

В соответствии с вариантом n = 632, m = 663. Результат работы программы представлен на Рис. 2.

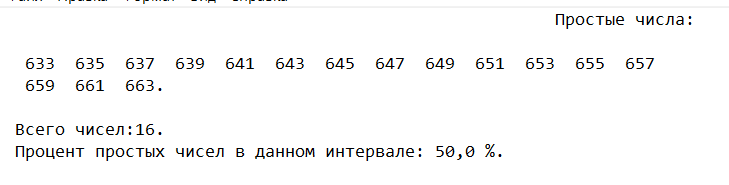


Рис.2 Результат нахождения простых чисел из диапазона [m;n] в программе L\_PROST

Ручные вычисления привели к количеству равному 6: 641, 643, 647, 653, 659, 661.

**3. Записать числа m и n в виде произведения простых множителей (форма записи – каноническая).**

632 = 2\*2\*79;

663 = 3\*13\*17;

**4. Проверить, является ли число, состоящее из конкатенации цифр m ǀǀ n (табл. 1.2), простым**

632663 – составное число. Оно имеет следующие делители: 37, 17099.

**5. Найти НОД (m, n).**

НОД(632, 663)

663 = 632 \* 1 + 31

632 = 31\*20 + 12

31 = 12 \* 2 + 7

12 = 7 \* 1 + 4

7 = 4 \* 1 + 3

4 = 3 \* 1 + 1

3 = 1 \* 3 + 0

НОД(632, 663) = 1

**6. Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:**

**• вычислять НОД двух либо трех чисел;**

**• выполнять поиск простых чисел.**

Результат вычисления НОД трех чисел изображен на Рис. 3.

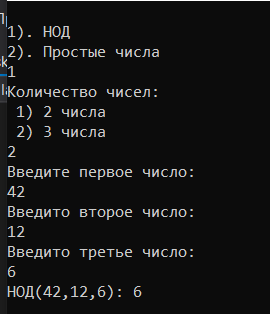


Рис.3 Результат нахождения НОД трех чисел

Результат поиска простых чисел от 2 до 35 изображен на Рис. 4.

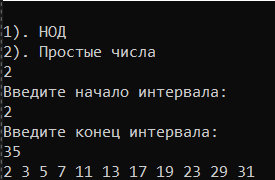


Рис.4 Результат нахождения простых чисел

**7. С помощью созданного приложения выполнить задания по условиям п. 1 и 2.**

Результаты п. 1 изображены на Рис. 5.

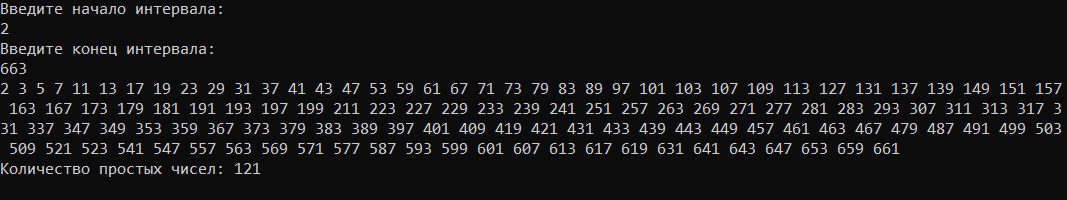


Рис.5 Результат нахождения простых чисел из диапазона [2;n]

Результаты п. 2 изображены на Рис. 6.

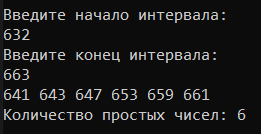


Рис.6 Результат нахождения простых чисел из диапазона [m;n]

**Вывод:** В ходе лабораторной работы я изучил такие алгоритмы как «решето Эратосфена», алгоритм Евклида, расширенный алгоритм Евклида. Была разработана программа по вычислению НОД чисел и поиску простых чисел из диапазона.