Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Лабораторная работа № 3**

«Основы теории чисел и их использование в криптографии»

Выполнил:

Студент: Лысков К.Е.

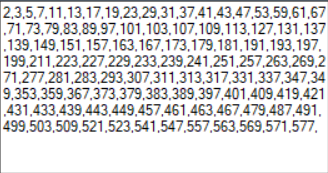
ФИТ 3 курс 4 группа

Преподаватель: Копыток Д.В.

Минск 2023

1) Используя L\_PROST, найти все простые числа в интервале [2, n]. Значение n соответствует варианту из табл. 1.2, указанному преподавателем. Подсчитать количество простых чисел в указанном интервале. Сравнить это число с n/ln(n) (см. выше пример 15).

n = 577;

****

Количество простых чисел в интервале [0,577]: 106.

577 / ln(577) = 90,7540602

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

m=540

Количество простых чисел в интервале [521,553]: 7.



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

n = 577

577= 577

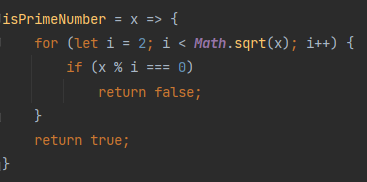
m =540

540 = 2\*2\*5\*3\*3\*3

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

540577

Для решения этого задания была разработана функция, которая проверяет остаток от деления числа 540577 на каждое число из промежутка [2, √540576].



Число является простым.

5) Найти НОД (540, 577).

577 = 540\*1 + 37;

540 = 37\*14 + 22;

37 = 22\*1 + 15;

22 = 15\*1 + 7;

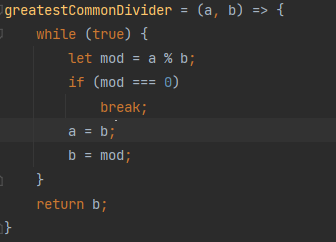
15 = 7\*2 + 1;

7 = 7\*1 + 0;

НОД(540;577) = 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.

Функция вычисляющие НОД для 2-х чисел:

****

Функция выполняющая поиск простых чисел:

