Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Основы теории чисел и их использование в криптографии.**

Студент: Плотников Д.А.

ФИТ 3 курс 5 группа

Преподаватель: Берников В.О.

Минск 2020

1. **Описание приложения**

В соответствии с целями лабораторной работы было создано приложение, обладающее следующим функционалом: расчет наибольшего общего делителя двух чисел, поиск простых чисел в указанном промежутке стандартным алгоритмом, поиск простых чисел в промежутке с помощью алгоритма «Решето Эратосфена» с отображением всех шагов, поиск коэффициентов соотношения Безу с помощью расширенного алгоритма Евклида. В приложении функционал разбит на именованные спойлеры, которые можно увидеть на рисунке 1.1.

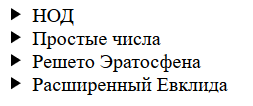


Рисунок 1.1 – Функции на главной странице приложения.

Название каждого пункта представляет собой задачу, которую содержимый этим пунктом интерфейс решает.

Первый пункт находит наибольший общий делитель двух чисел, получаемых из текстовых полей, а результат появится в следующем текстовом поле. Как это выглядит можно увидеть на рисунке 1.2.

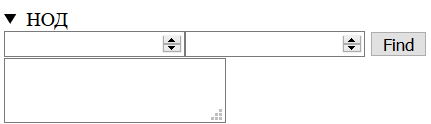


Рисунок 1.2 – Интерфейс, для расчета НОД двух чисел.

Второй пункт меню дает возможность получить простые числа из заданного интервала и отобразить их в табличном виде, при этом так же производится расчет количества простых чисел по приблизительной формуле. Увидеть интерфейс можно на рисунке 1.3.



Рисунок 1.3 – Интерфейс, для поиска простых чисел на промежутке.

Третий пункт сходу может показаться аналогичным второму, за исключением того, что каждый шаг прохода алгоритмом «Решето Эратосфена» выводится отдельной строкой, интерфейс можно рассмотреть на рисунке 1.4.



Рисунок 1.4 – Интерфейс, для поиска простых чисел в промежутке.

Последний пункт меню позволяет произвести расчет коэффициентов соотношения Безу, через которые выражается НОД этих же двух чисел. Интерфейс, посредством которого решается задача предоставлен на рисунке 1.5.

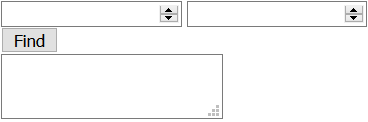


Рисунок 1.5 – Интерфейс, для поиска коэффициентов Безу.

# 2. Методика выполнения расчетов

Условие по варианту представляет собой два числа m и n, значение которых предоставлены на рисунке 2.1.



Рисунок 2.1 – Числа, выбранные для расчетов.

Рассчитаем НОД, выбранных чисел с помощью разработанного приложения. Для этого нужно ввести числа в соответствующие поля и нажать кнопку. Результат выполнения предоставлен на рисунке 2.2.

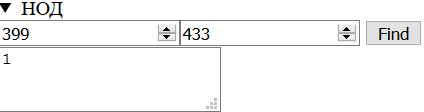


Рисунок 2.2 – Результат расчета НОД двух чисел в программе.

Так наибольший общий делитель двух чисел оказался равен единице, то можно сделать вывод, что числа являются взаимно простыми.

Далее, стоит найти все простые числа, находящиеся в указанном промежутке, результат выполнения предоставлен на рисунке 2.3.

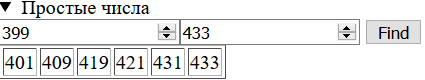


Рисунок 2.3 – Результат поиска простых чисел.

Очень важным является момент поиска количества простых чисел, стоит попробовать найти их количество от 1 до 433, и сравнить с расчетным значением. Результат выполнения предоставлен на рисунке 2.4.

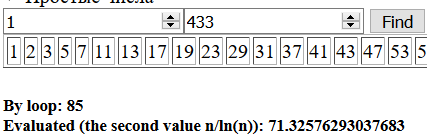


Рисунок 2.4 – Результат вычисления количества простых чисел.

Таким образом можно сделать вывод о том, что формула лишь примерно дает оценку количеству простых чисел.

Количество можно сравнить с тем же промежутком, но посчитанным с помощью алгоритма «Решето Эратосфена», результат расчета которого представлен на рисунке 2.5.

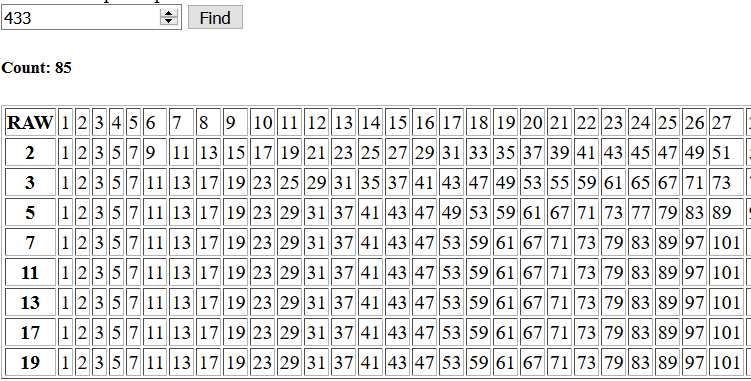


Рисунок 2.5 – Результат выполнения алгоритма «Решето Эратосфена».

В результате выполнения можно увидеть каждый прогон по массиву в виде отдельной строки. Таким образом на последней строке остаются лишь простые числа.

Теперь стоит попробовать рассчитать коэффициенты соотношения Безу с помощью расширенного алгоритма Евклида. Результат выполнения предоставлен на рисунке 2.6.

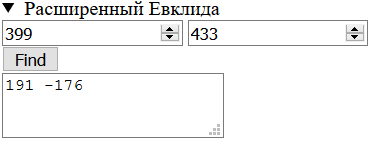


Рисунок 2.6 – Результат работы расширенного алгоритма Евклида.

**Вывод**

В ходе этой работы были приобретены навыки выполнения операций с числами для решения задач в области криптографии. Были изучены: алгоритм Евклида, решето Эратосфена, расширенный алгоритм Евклида, свойства простых чисел и их роль в области криптографии.

Было разработано приложение на языках js и c++ для автоматизации операций с числами для решения задач в области криптографии.