МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №3**

**«Основы теории чисел и их использование в криптографии»**

Выполнил:

студент 3 курса 5 группы

Храмых В. О.

Проверила: Блинова Е. А.

Минск 2020

Цель: приобретение практических навыков выполнения операций с числами для решения задач в области криптографии и разработка приложений для автоматизации этих операций.

Задачи:

* Закрепить теоретические знания по высшей арифметике.
* Научиться практически решать задачи с использованием простых и взаимно простых чисел, вычислений по правилам модулярной арифметики и нахождению обратных чисел по модулю.
* Ознакомиться с особенностями реализации готового программного средства L\_PROST и особенностями выполнения с его помощью операций над простыми числами.
* Разработать приложение для реализации указанных преподавателем операций с числами.
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

В результате данной лабораторной работы было создано приложение для вычисления наибольшего общего делителя для двух и трех чисел, а также подсчета количества простых чисел в интервале.

Реализация функции для вычисления наибольшего общего делителя представлена на рисунке 1.

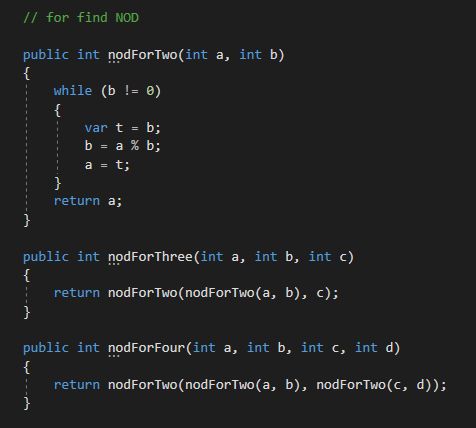


Рисунок 1 – функция для вычисления наибольшего общего делителя

Результат вычисления НОД для двух и трех чисел представлен на рисунках 2 и 3.

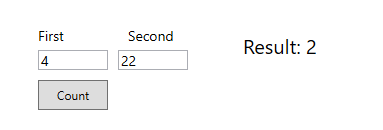


Рисунок 2 – результат вычисления НОД для двух чисел

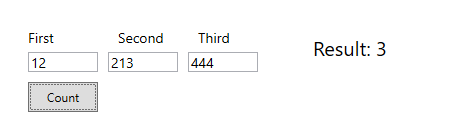


Рисунок 3 – результат вычисления НОД для трех чисел

Реализация функции для нахождения простых чисел представлена на рисунке 4.

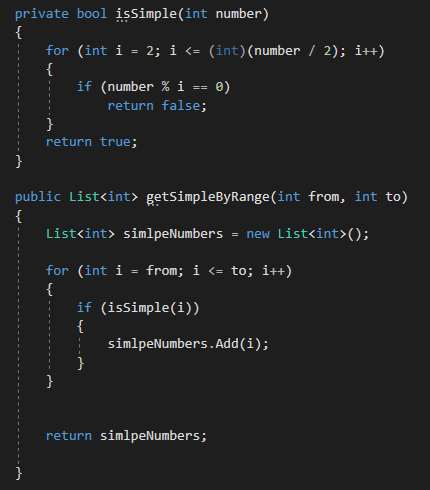


Рисунок 4 – реализация функции нахождения простых чисел

По заданию лабораторной работы необходимо найти все простые числа, а также их количество, в интервале [2, n], где n соответствует варианту из таблицы, в данном случае вариант 12 (n = 521, m = 553). Результат выполнения задания представлен на рисунке 5.

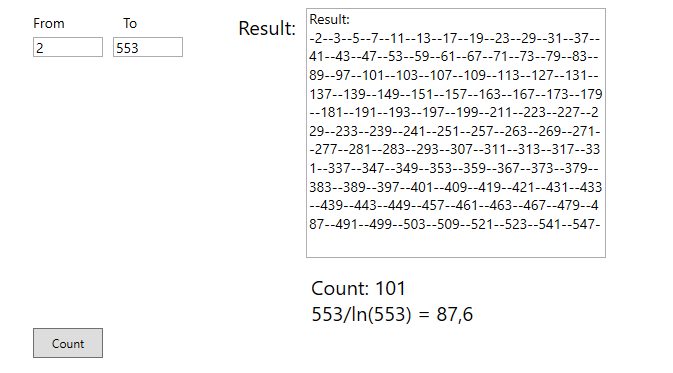


Рисунок 5 – простые числа в интервале [2, 397]

Подсчитаем n/ln(n): 553/ln(553) ≈ 87.6, реальное количество простых чисел немного больше.

Найдем все простые числа в интервале [m, n], т.е. [521, 553]. Результаты представлены на рисунке 6.

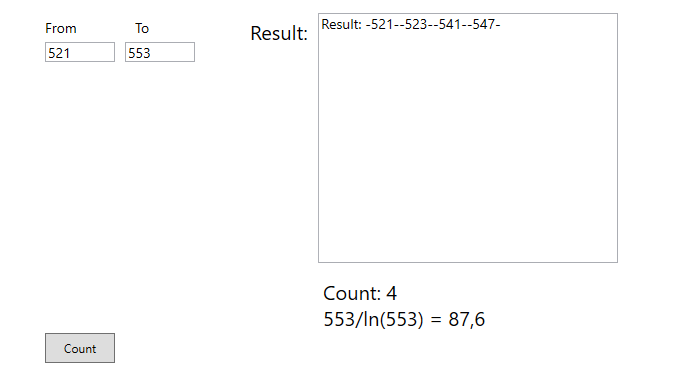


Рисунок 6 – простые числа в интервале [521, 553]

Для сравнения посчитаем «вручную», используя «решето Эратосфена»:

Шаг 1. Выпишем числа от 521 до 553:

521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553

Шаг 2. Удалим из списка числа кратные 2:

521, 523, 525, 527, 529, 531, 533, 535, 537, 539, 541, 543, 545, 547, 549, 551, 553.

Шаг 3. Удалим из списка числа кратные 3:

521, 523, 527, 529, 533, 535, 539, 541, 545, 547, 551, 553,

Шаг 4. Удалим из списка числа кратные 5:

521, 523, 527, 529, 533, 539, 541, 547, 551, 553.

Шаг 5. Удалим из списка числа кратные 7:

521, 523, 527, 529, 533, 541, 547, 551.

Шаг 6. Удалим из списка числа кратные 11:

521, 523, 527, 529, 533, 541, 547, 551.

Шаг 7. Удалим из списка числа кратные 13:

521, 523, 527, 529, 541, 547, 551.

Шаг 8. Удалим из списка числа кратные 17:

521, 523, 529, 541, 547, 551.

Шаг 9. Удалим из списка числа кратные 19:

521, 523, 529, 541, 547.

Шаг 10. Удалим из списка числа кратные 23:

521, 523, 541, 547.

Шаг 11. Удалим из списка числа кратные 29:

521, 523, 541, 547.

Шаг 12. Удалим из списка числа кратные 31:

521, 523, 541, 547.

По результатам вычисления получили такие же 4 чисел.

Также в ходе лабораторной работы, необходимо было разработать функцию для нахождения числа обратного по модулю, реализация данной функции представлена на рисунке 7.

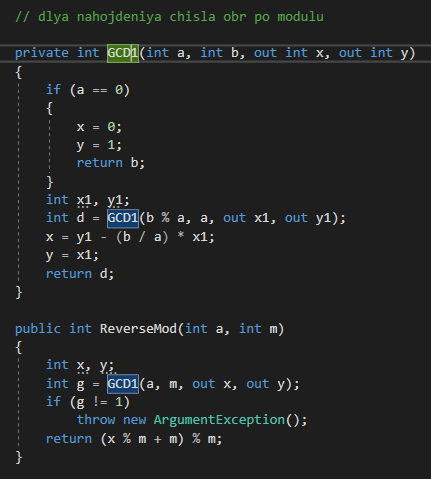


Рисунок 7 – реализация функции вычисления обратного числа по модулю

На рисунке 8 представлены примеры работы функции для расчета обратного числа по модулю, в разработанном приложении.

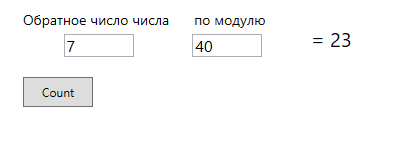


Рисунок 8 – пример работы функции нахождения обратного числа по модулю

Вывод: в ходе данной лабораторной работы, было разработано приложение для вычисления наибольшего общего делителя для двух и трёх чисел, а также реализована возможность поиска простых чисел в заданном диапазоне и вычисления обратного числа по модулю. Также были проведены «ручные» расчёты, для сравнения с полученными результатами из программы.