МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №3**

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

Выполнила студентка 3 курса 5 группы Максимчикова Ю. С.

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.
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.
* 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 расчета НОД двух либо трех чисел, а также для поиска простых чисел.

В первом задании данной лабораторной работы необходимо было найти все простые числа в интервале [2, n], используя самостоятельно разработанное программное средство. Значение n выбирается из таблицы в соответствии с вариантом. Для варианта номер 11 значение n равняется 591. Программный код, реализующий алгоритм для поиска всех простых чисел в интервале, представлен на рисунке 1.

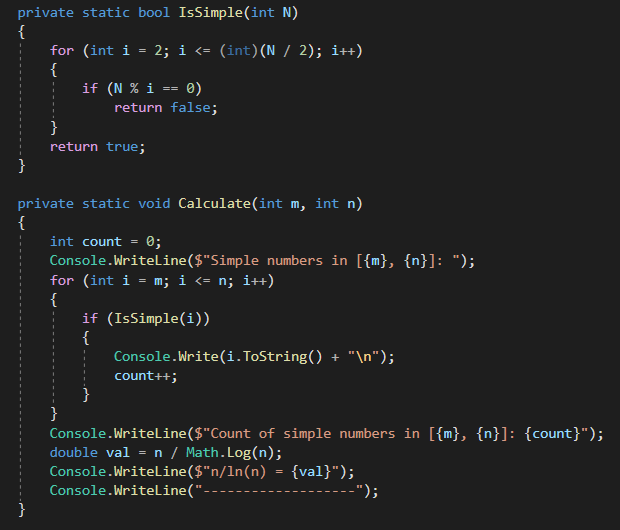


Рис. 1 – Программный код, реализующий алгоритм для поиска всех простых чисел в интервале

Результаты поиска простых чисел в интервале [2, 591] представлены ниже на рисунке 2.

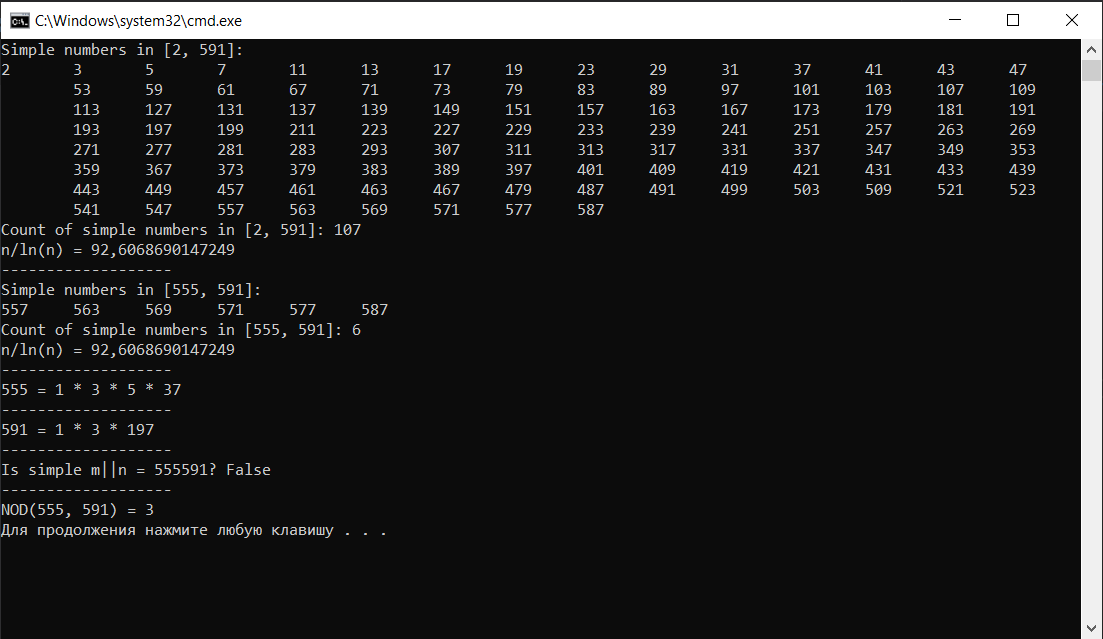


Рис. 2 – Результаты поиска простых чисел в интервале [2, 591]

Вспомним одно из свойств простых чисел и посмотрим, как оно «работает» для нашего примера. Вычислим n/ln(n) =591/ ln591 ≈ 92,6. Результат (с учетом округления до целого) не совсем близок к истинному: количеству простых чисел от 1 до n =591.

Во втором задании данной лабораторной работы необходимо было найти все простые числа в интервале [m, n], используя самостоятельно разработанное программное средство. Значения m и n выбираются из таблицы в соответствии с вариантом. Для варианта номер 11 значение n равняется 591, а значение m - 555. Результаты поиска простых чисел в интервале [555, 591] представлены ниже на рисунке 3.

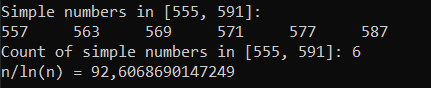


Рис. 3 – Результаты поиска простых чисел в интервале [555, 591]

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

Шаг 1. Выпишем числа от 555 до 591:

555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591.

Шаг 2. Удалим из списка числа кратные 2:

555, 557, 559, 561, 563, 565, 567, 569, 571, 573, 575, 577, 579, 581, 583, 585, 587, 589, 591.

Шаг 3. Удалим из списка числа кратные 3:

557, 559, 563, 565, 569, 571, 575, 577, 581, 583, 587, 589.

Шаг 4. Удалим из списка числа кратные 5:

557, 559, 563, 569, 571, 577, 581, 583, 587, 589.

Шаг 5. Удалим из списка числа кратные 7:

557, 559, 563, 569, 571, 577, 583, 587, 589.

Шаг 6. Удалим из списка числа кратные 11:

557, 559, 563, 569, 571, 577, 587, 589.

Шаг 7. Удалим из списка числа кратные 13:

557, 563, 569, 571, 577, 587, 589.

Шаг 8. Удалим из списка числа кратные 17:

557, 563, 569, 571, 577, 587, 589.

Шаг 9. Удалим из списка числа кратные 19:

557, 563, 569, 571, 577, 587.

По результатам вычисления получили такие же 6 чисел.

В третьем задании данной лабораторной работы необходимо было записать числа m и n в виде произведения простых множителей (форма записи – каноническая), используя самостоятельно разработанное программное средство. Программный код, реализующий алгоритм для записи числа в виде произведения простых множителей, представлен на рисунке 4.

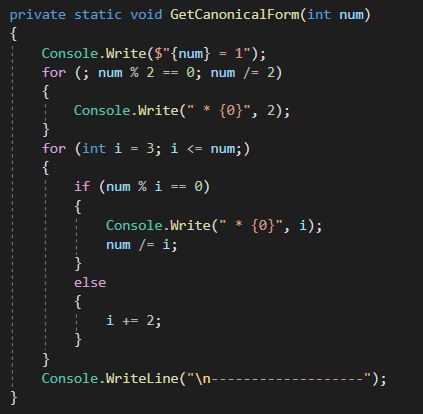


Рис. 4 – Программный код, реализующий алгоритм для записи числа в виде произведения простых множителей

Результат работы программного средства для записи чисел m и n в виде произведения простых множителей представлен ниже на рисунке 5.

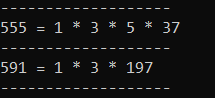


Рис. 5 – Представления чисел m и n в виде произведения простых множителей

В четвертом задании данной лабораторной работы необходимо было проверить, является ли число, состоящее из конкатенации цифр чисел m и n, простым. Результат работы программного средства представлен на рисунке 6.



Рис. 6 – Результат работы программного средства

В пятом задании данной лабораторной работы необходимо было найти наибольший общий делитель (НОД) чисел m и n. Для поиска НОД двух чисел в программе был использован алгоритм Евклида.

Программный код, реализующий алгоритм Евклида, представлен на рисунке 7.

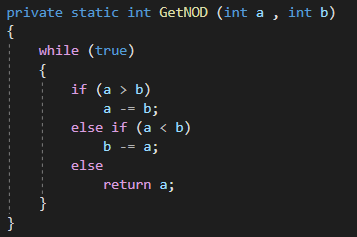


Рис. 7 – Программный код, реализующий алгоритм Евклида

Результат вычисления НОД чисел m и n представлен ниже на рисунке 8.



Рис. 8 – Наибольший общий делитель чисел 555 и 591

Вывод: в результате данной лабораторной работы было разработано приложение для поиска простых чисел и вычисления числа, обратного к числу по модулю. Также данная лабораторная работа помогла закрепить 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.