Учреждение образования

«Белорусский государственный технологический университет»

**Отчет по лабораторной работе №3**

по дисциплине: «Информационная безопасность»

Студента 3 курса 6 группы ФИТ

Гвоздовского Кирилла Владимировича

**Лабораторная работа №3**

**Оcновы теории чисел и их использование в криптографии**

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

**Задачи:**

1. Закрепить теоретические знания по высшей арифметике.

2. Научиться практически решать задачи с использованием простых и взаимно простых чисел, вычислений по правилам модулярной арифметики и нахождению обратных чисел по модулю.

3. Ознакомиться с особенностями реализации готового программного средства L\_PROST и особенностями выполнения с его помощью операций над простыми числами.

4. Разработать приложение для реализации указанных преподавателем операций с числами.

5. Результатывыполнения лабораторной работыоформить в виде описания разработанного приложения, методики выполнения эксперимента с использованием приложения и результатов эксперимента.

**Теоретические сведения**

В основе современной криптографии лежит теория чисел. Теория чисел, или высшая арифметика, – раздел математики, изучающий натуральные числа и иные похожие величины. В зависимости от используемых методов в теории чисел рассматривают несколько направлений. Нас будут интересовать вопросы делимости целых чисел, вычисления наибольшего общего делителя (НОД), разложение числа на простые множители, малая теорема Ферма́, теорема Эйлера, элементы теории вычетов.

Делимость – одно из основных понятий теории чисел. Если для некоторого целого числа a и натурального числа b существует целое число q, при котором bq = a, то говорят, что число a делится на b. В этом случае b называется делителем числа a, а a называется кратным числу b. При этом используются следующие обозначения:

a ⋮ b – a делится на b, или b | a – b делит a.

Из последнего определения следует, что:

• любое натуральное число является делителем нуля;

• единица является делителем любого целого числа;

• любое натуральное число является делителем самого себя.

Если число не имеет делителей, кроме самого себя и единицы, то оно называется **простым**, а если у числа есть еще делители, то **составным**.

Если два простых числа отличаются на 2, то их называют **числами-близнецами**. Таких чисел не очень много. Например, ими являются 5 и 7, 29 и 31, 149 и 151.

Наибольшее целое число, которое делит без остатка числа a и b, называется **наибольшим общим делителем** этих чисел – НОД (a, b).

**Взаимно простыми** являются целые числа, наибольший общий делитель которых равен 1.

Если НОД (a, b) = d, то справедливо следующее соотношение (**соотношение Безу**): аu + bv = d. Эта формула называется также реализацией «**расширенного алгоритма Евклида**». Этот алгоритм состоит из двух этапов: собственно алгоритма Евклида и вычислений на основе обратных подстановок или последовательного выражения остатков в каждом из шагов предыдущего этапа с соответствующим приведением подобных на каждом шаге.



Количество натуральных чисел, непревосходящих nивзаимно простых с n, называется **функцией Эйлера** и обозначается φ(n).

Если p – простое число, то φ(p) = p – 1, если числа p и q являются простыми и p ≠ q, то φ(p) = (p – 1)(q – 1).

**Ход работы**

Код программы на языке JavaScript, реализующий задание №1, представлен ниже.

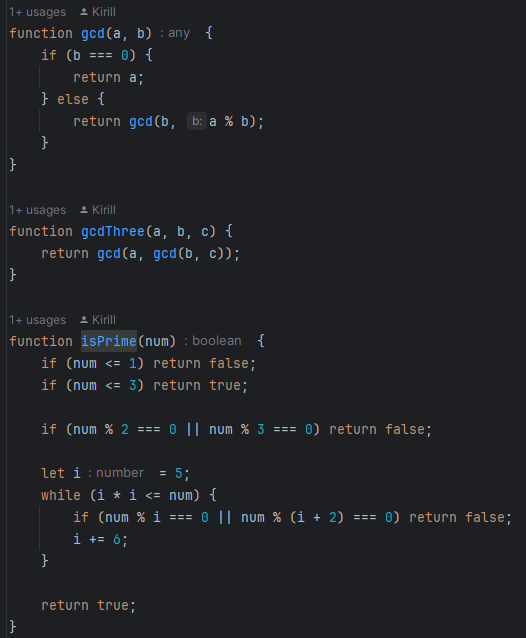


Рисунок 1 – Код программы

Код программы на языке JavaScript, реализующий задание №2, представлен ниже на рисунке 2.

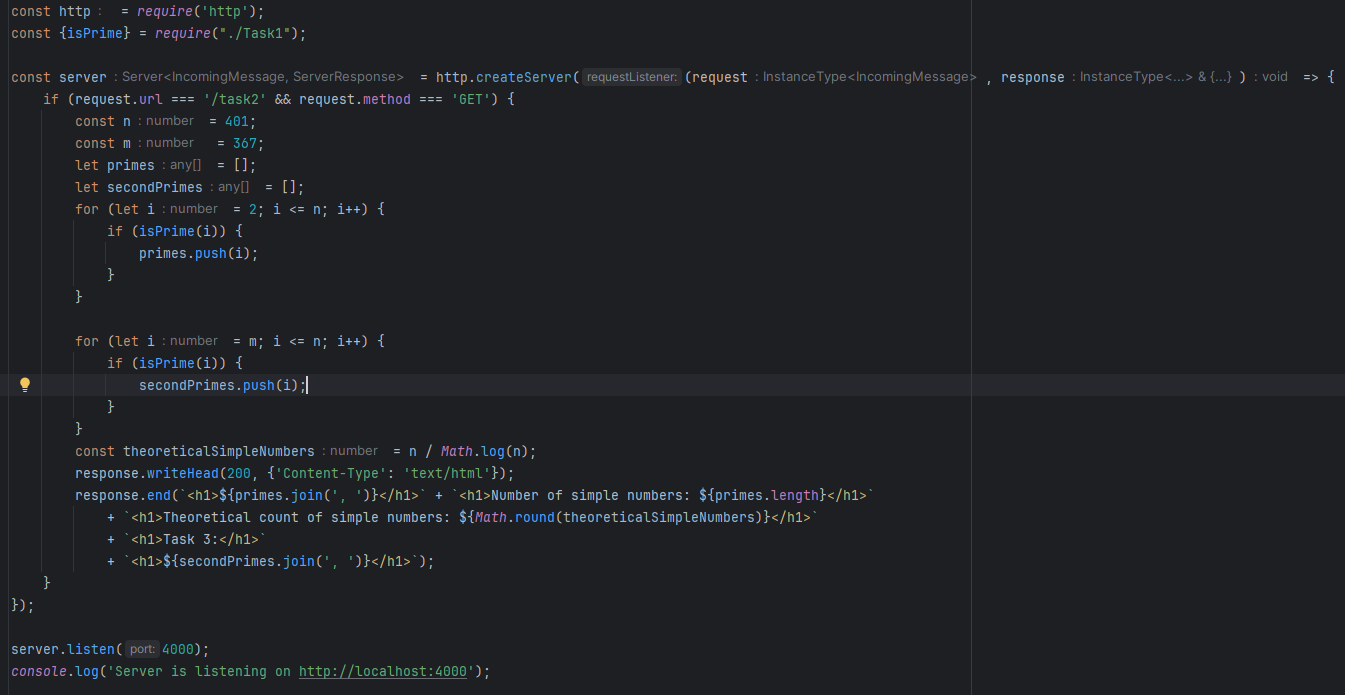


Рисунок 2 – Код программы для задания №2



Рисунок 3 — Результат выполнения задания №1

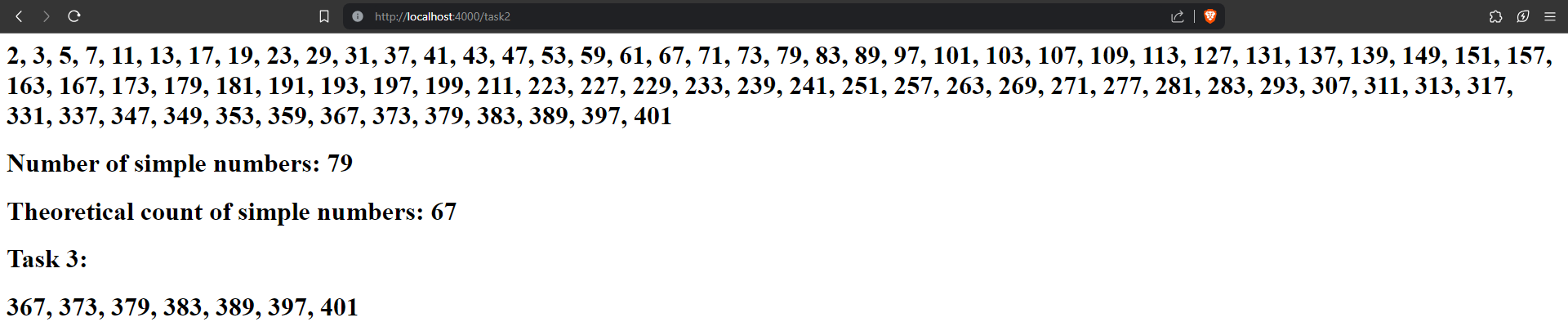


Рисунок 4 — Результат выполнения задания №2

Следующим шагом нужно было сравнить полученные результаты с «ручными» вычислениями, используя «решето Эратосфена» на промежутке [367; 401]. Для этого выполним следующие шаги:

1. Выпишем числа от 367 до 401:

367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401.

1. Воспользуемся свойством 3 простых чисел и вычислим , т. е. меньше 20.
2. Удалим последовательно все числа, делящиеся на простые числа от 2 до 20. Такими простыми числами являются: 2, 3, 5, 7, 11, 13, 17, 19.

Числа, которые делятся на 2: 368, 370, 372, 374, 376, 378, 380, 382, 384, 386, 388, 390, 392, 394, 396, 398, 400.

Оставшиеся числа: 367, 369, 371, 373, 375, 377, 379, 381, 383, 385, 387, 389, 391, 393, 395, 397, 399, 401.

Числа, которые делятся на 3: 369, 375, 381, 387, 393, 399.

Оставшиеся числа: 367, 371, 373, 377, 379, 383, 385, 389, 391, 395, 397, 401.

Числа, которые делятся на 5: 385, 395.

Оставшиеся числа: 367, 371, 373, 377, 379, 383, 389, 391, 397, 401.

Числа, которые делятся на 7: 371.

Оставшиеся числа: 367, 373, 377, 379, 383, 389, 391, 397, 401.

Числа, которые делятся на 13: 377.

Оставшиеся числа: 367, 373, 379, 383, 389, 391, 397, 401.

Числа, которые делятся на 17: 391.

Оставшиеся числа: 367, 373, 379, 383, 389, 397, 401.

Числа, которые делятся на 19: 389.

Оставшиеся числа: 367, 373, 379, 383, 397, 401.

В итоге, после выполнения всех операций в «решете» останутся числа: 367, 373, 379, 383, 389, 397, 401. Эти числа совпадают с найденными ранее простыми числами на промежутке [367, 401].

**Вывод:** В ходе лабораторной работы были приобретены навыки выполнения операций с числами для решения задач в области криптографии, а также разработано приложение для автоматизации этих операций.