Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Лабораторная работа №3

**ОСНОВЫ ТЕОРИИ ЧИСЕЛ И ИХ ИСПОЛЬЗОВАНИЕ В КРИПТОГРАФИИ**

Студент: Сосновец М.И.

ФИТ 3 курс 4 группа

Преподаватель: Нистюк О.А.

Минск 2025

**Цель**: приобретение практических навыков выполнения операций с числами для решения задач в области криптограф

**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. Результаты выполнения лабораторной работы оформить 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.

**Определение 1.** Множество всех целых чисел (обозначим буквой Z) есть набор всех действительных чисел без дробной части: {..., –3, –2, –1, 0, 1, 2, 3, ...}.

**Определение 2.** Натуральные числа являются подмножеством целых чисел и образуют множество N: {1, 2, 3, ...}.

**Определение 3.** 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. **Определение 4.** Делитель a называется собственным делителем числа b, если 1 < |a| < |b|, и несобственным – в противном случае.

**Определение 5.** Всякое целое число а можно представить с помощью положительного целого числа b равенством вида а = bq + r, 0 ≤ r ≤ b. Число q называется неполным частным, а число r – остатком отделения а на b.

**Определение 6.** Натуральное число n называется простым, если n > 1 и не имеет положительных делителей, отличных от 1 и n. Простое число не делится без остатка ни на одно другое число.

Основная теорема арифметики. Всякое натуральное число n, кроме 1, можно представить как произведение простых множителей:

n = p1p2p3...pz, z > 1.

**Определение 7**. Натуральное число n называется составным, если n > 1 и имеет по крайней мере один положительный делитель, отличный от 1 и n.

**Определение 8.** 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. Всякое натуральное число n > 1 либо является простым числом, либо имеет простой делитель

Понятие делимости чисел (см. определение 3) является одним из важных в теории чисел. С этим понятием, а также с его производным – общим делителем (см. определение 4) связаны другие важнейшие (в частности, для криптографии) понятия: наибольшего общего делителя (НОД) и взаимно простых чисел.

**Определение 9.** Наибольшее целое число, которое делит без остатка числа a и b, называется наибольшим общим делителем этих чисел – НОД (a, b).

**Определение 10.** Взаимно простыми являются целые числа, наибольший общий делитель которых равен 1.

**Практическое задание**

1. Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:

• вычислять НОД двух либо трех чисел;

• выполнять поиск простых чисел.

2. Используя приложение, 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).

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

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

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

6. Найти НОД (m, n).

7. Результаты выполнения работы оформить в виде отчета по установленным правилам.

**Задание 1:**

Было разработано приложение, которое позволяет находить простые числа и вычислять наибольший общий делитель (НОД) как для двух, так и для трех чисел. Алгоритм для проверки простого числа представлен в листинге 1.1

|  |
| --- |
| const isPrime = (num) => {          if (num < 2) return false;          for (let i = 2; i <= Math.sqrt(num); i++) {              if (num % i === 0) return false;          }          return true;      }; |

Листинг 1.1 – Реализация функции нахождения простого числа

На рисунке 1 показан результат выполнения поиска простого числа заданного диапазона.

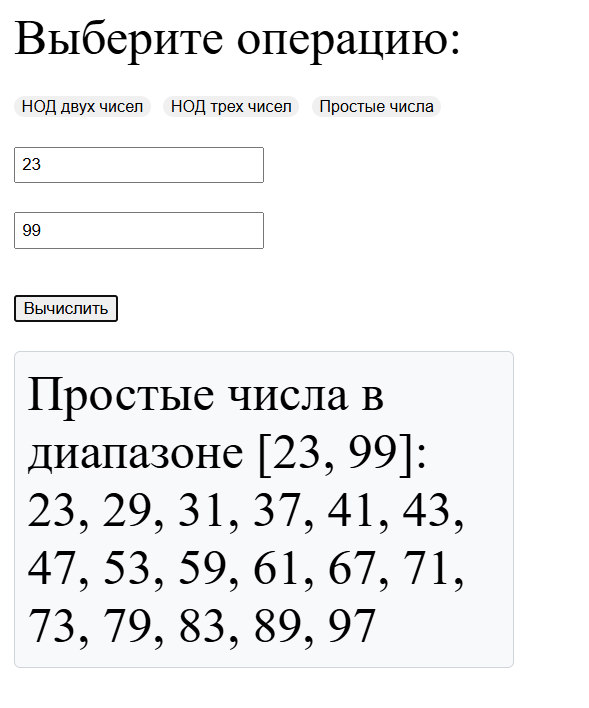


Рисунок 1 – Результат поиска простых чисел в диапазоне

Алгоритм для нахождения наибольшего общего делителя двух чисел представлен в листинге 1.2

|  |
| --- |
| const gcdTwoNumbers = (a, b) => {          while (b !== 0) {              [a, b] = [b, a % b];          }          return a;      }; |

Листинг 1.2 – Реализация функции нахождения наибольшего общего делителя двух чисел

На рисунке 2 показан результат выполнения нахождения наибольшего общего делителя (НОД) двух чисел.

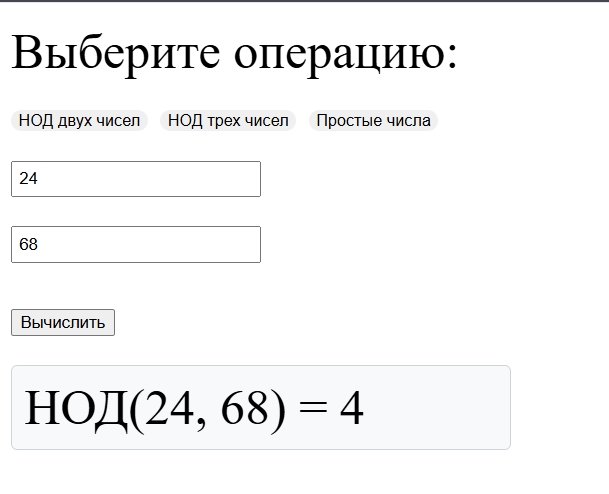


Рисунок 2 – Результат вычисления НОД для двух чисел

Алгоритм для нахождения наибольшего общего делителя трех чисел представлен в листинге 1.3

|  |
| --- |
| const gcdThreeNumbers = (a, b, c) => gcdTwoNumbers(gcdTwoNumbers(a, b), c); |

Листинг 1.3 – Реализация функции нахождения наибольшего общего делителя трех чисел

На рисунке 3 показан результат выполнения нахождения наибольшего общего делителя (НОД) трех чисел.

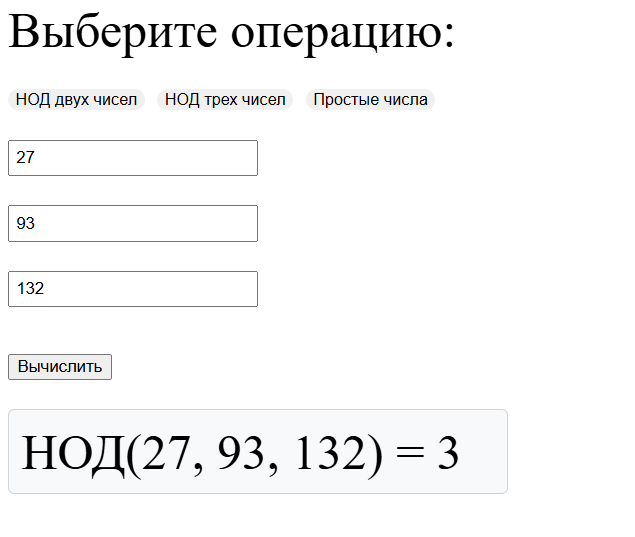


Рисунок 3 – Результат вычисления НОД для трех чисел

В рамках данного задания было разработано приложение, которое позволяет находить простые числа и вычислять наибольший общий делитель (НОД) как для двух, так и для трех чисел.

**Задание 2:**

Используя приложение были найдены все простые числа в интервале [2, n], где n равняется 397. Результат представлен на рисунке 4.

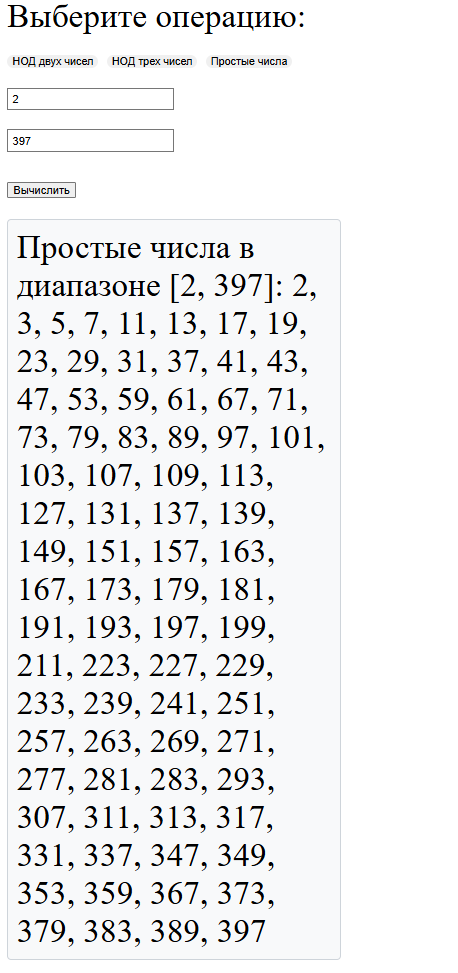


Рисунок 4 – Результат поиска простых чисел в диапазоне [2, 397]

В диапазоне от 2 до 397 располагается 78 простых чисел.

Сравнение 78 и 78/ln(78). Результат предоставлен на рисунке 5.

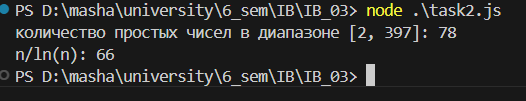


Рисунок 5 – Результат 78 и 78/ln(78)

Таким образом, теоретическая оценка достаточно близка к реальному значению, но реальное количество простых чисел немного выше, что также ожидаемо для этого диапазона.

**Задание 3:**

Результат поиска простых чисел в диапазоне [354, 397] представлен на рисунке 6.

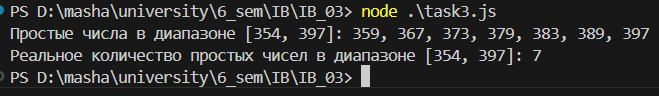


Рисунок 6 – Результат поиска простых чисел в диапазоне [354, 397]

Теперь сравним полученные результаты с «ручными» вычислениями, используя «решето Эратосфена». Результат вычисления представлен на рисунке 7.

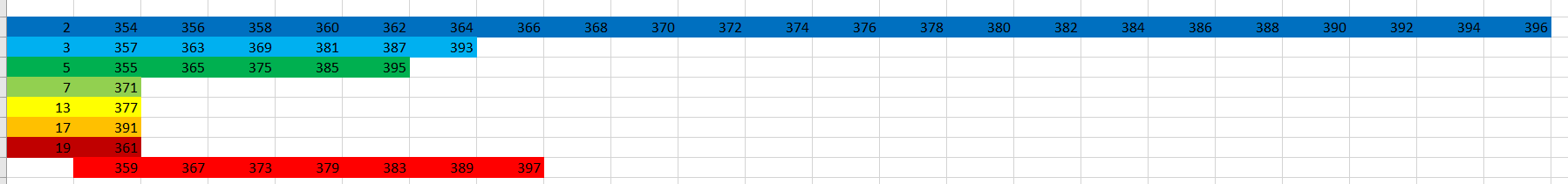


Рисунок 7 – Результат вычисления

**Задание 4:**

В задании реализована функция разложения целых чисел m и n на простые множители в канонической форме. Каноническая форма записи числа — это его представление как произведения простых чисел с соответствующими степенями. Результат выполнения представлен на рисунке 8.

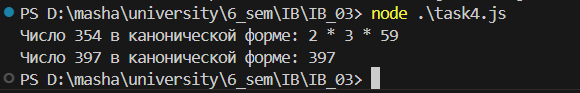


Рисунок 7 – 354 и 397 в виде произведения простых множителей

**Задание 5:**

Проверка, является ли число, состоящее из конкатенации цифр 354 ǀǀ 397, простым представлена на рисунке 8.

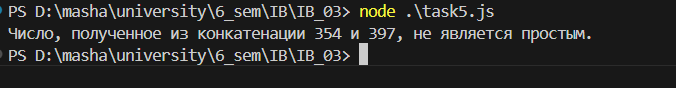


Рисунок 8 – Проверка, является ли число, состоящее из конкатенации цифр 354 ǀǀ 397, простым

Число 354397 имеет делители, кроме 1 и самого себя, следовательно, оно не является простым. Пример делителя — это число 7, которое делит 354397 нацело

**Задание 6:**

НОД чисел 354 и 397 представлен на рисунке 9.

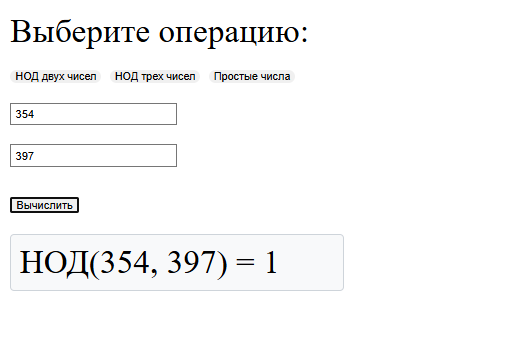


Рисунок 8 – НОД чисел 354 и 397

**Вывод:**

В этой лабораторной работе были получены практических навыков выполнения операций с числами для решения задач в области криптографии и разработка приложений для автоматизации этих операций. Был освоен метод ручного поиска простых чисел «решето Эратосфена».