Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Лабораторная работа №3

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

Студент: Чёрная Я.Р.

ФИТ 3 курс 4 группа

Преподаватель: Нистюк О.А.

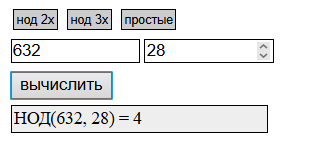
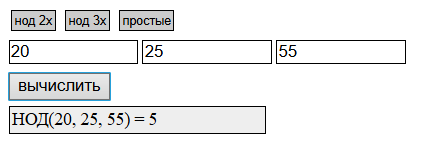
Минск 2025

**Задание 1:**

Разработано приложение, которое позволяет находить простые числа и вычислять наибольший общий делитель (НОД) как для двух, так и для трех чисел.

|  |
| --- |
| 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 – определение простое число или нет

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

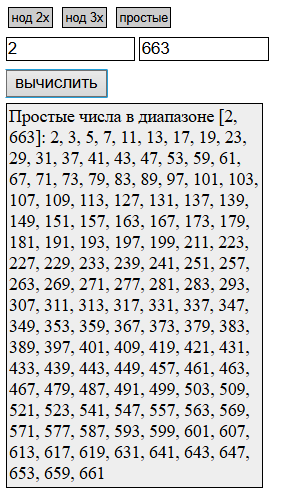
Листинг 1.2 – нахождение наибольшего общего делителя двух чисел

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

Листинг 1.3 – нахождение наибольшего общего делителя трех чисел

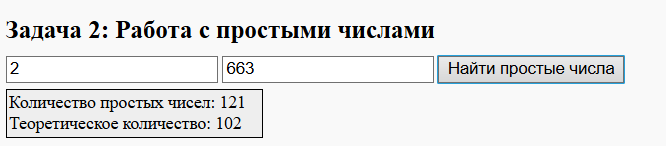
**Задание 2:**

Были найдены все простые числа в интервале [2, n].



В диапазоне от 2 до 663 располагается 121 простое число.

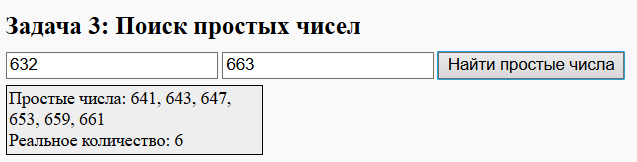
Сравнение 121 и 121/ln(121).



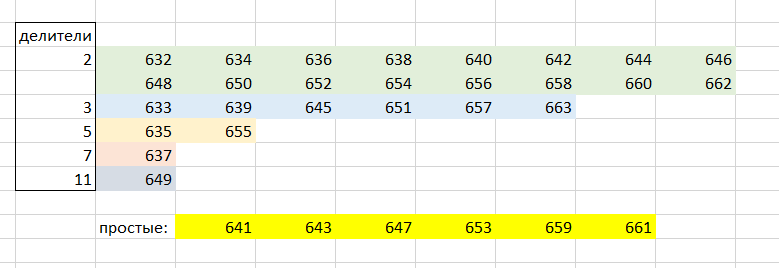
Теоретическая оценка достаточно близка к реальному значению, но реальное количество простых чисел немного выше.

**Задание 3:**

Поиск простых чисел в диапазоне [632, 397].

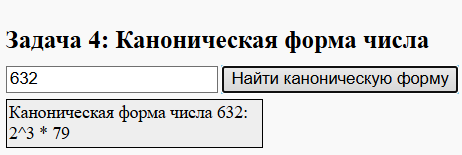


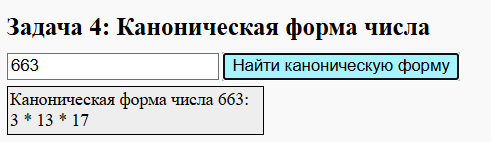
Теперь сравним полученные результаты с «ручными» вычислениями, используя «решето Эратосфена».



**Задание 4:**

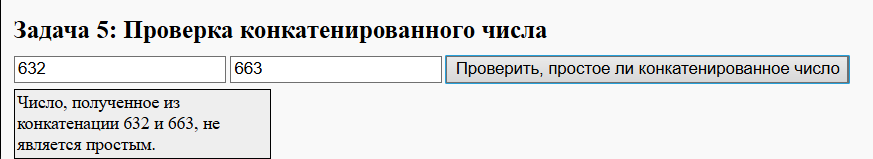
В задании реализована функция разложения целых чисел m и n на простые множители в канонической форме. Каноническая форма записи числа — это его представление как произведения простых чисел с соответствующими степенями.



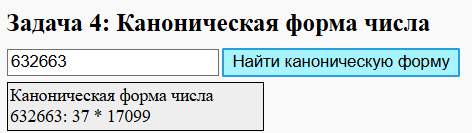


**Задание 5:**

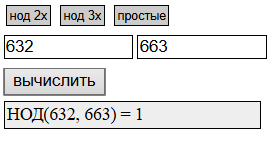
Проверка, является ли число, состоящее из конкатенации цифр 632 ǀǀ 663, простым



Можем это проверить с помощью предыдущего задания.



**Задание 6:**



**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.