МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы теории чисел и их использование в криптографии

Студент: Евсеенко В. П.

ФИТ 3 курс 4 группа

Преподаватель: Савельева М. Г.

Минск 2025

Содержание

[Введение 3](#_Toc192678812)

[1 Практическое задание 4](#_Toc192678813)

[Задание 1 4](#_Toc192678814)

[Задание 2 5](#_Toc192678815)

[Задание 3 6](#_Toc192678816)

[Задание 4 6](#_Toc192678817)

[Задание 5 6](#_Toc192678818)

[2 Основное задание 7](#_Toc192678819)

# **Введение**

Цель лабораторной работы:

* 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 эксперимента с использованием приложения и результатов эксперимента.

# **Практическое задание**

# **Задание 1**

Используя L\_PROST, найти все простые числа в интервале [2, *n*]. Значение n соответствует своему варианту из табл. 1.1, указанному преподавателем. Подсчитать количество простых чисел в указанном интервале. Сравнить это число с *n/*ln*(n).*

Таблица 1.1 – Варианты задания

|  |  |  |
| --- | --- | --- |
| Вариант | *m* | *n* |
| 1 | 450 | 503 |
| 2 | 521 | 553 |
| 3 | 367 | 401 |
| 4 | 421 | 457 |
| 5 | 499 | 531 |
| 6 | 431 | 471 |
| 7 | 540 | 577 |
| 8 | 667 | 703 |
| 9 | 399 | 433 |
| 10 | 587 | 621 |
| 11 | 555 | 591 |
| 12 | 354 | 397 |
| 13 | 379 | 411 |
| 14 | 632 | 663 |
| 15 | 447 | 477 |

Выбранный вариант – 4, следовательно *n* = 457. На рисунке 1.1 следующим образом отображено как в приложении L\_PROST будет производится поиск, там же указывается интервал, в представленном случае интервал будет [2, 457].

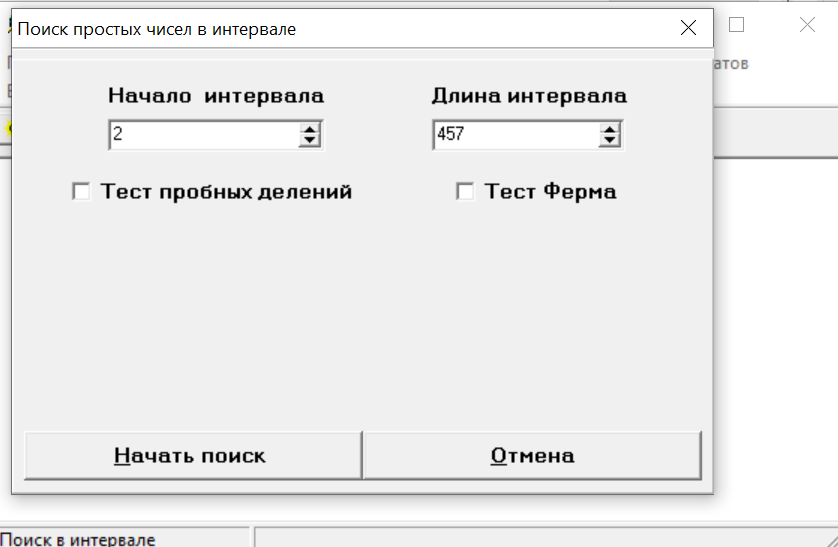


Рисунок 1.1 – Поиск простых чисел в заданном интервале

Результат поиска простых чисел представлен на рисунке 1.2.

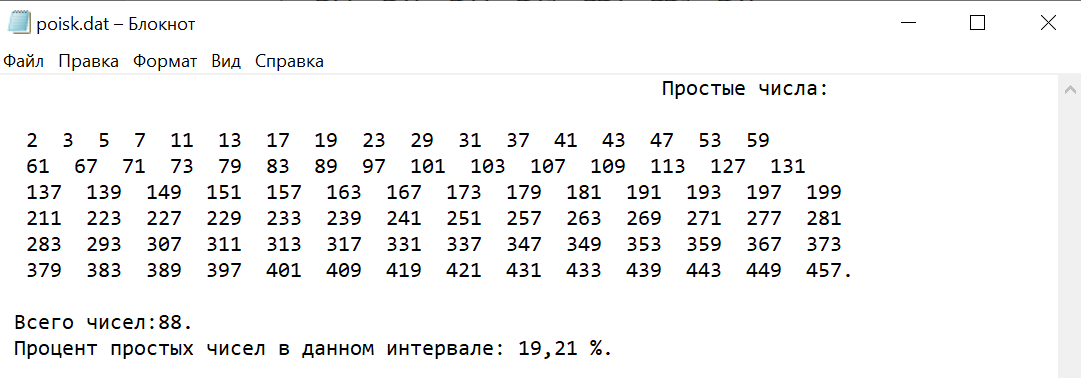


Рисунок 1.2 – Результат поиска простых чисел в заданном интервале

Общее количество простых чисел равняется 88, чтобы сравнить его с выражением *n/*ln*(n)*, посчитаем само выражение: 457/ln*(*457*)* ≈ 74,6161, НОД(88,74) = 2, следовательно числа не взаимно простые.

# **Задание 2**

Повторить задание 1 для интервала [*m, n*]. Сравнить полученные результаты с «ручными» вычислениями, используя «решето Эратосфена».

Значение *m* = 421, а значение *n* =457. Результат выполнения здания для интервала [421,457] представлен на рисунке 1.3.

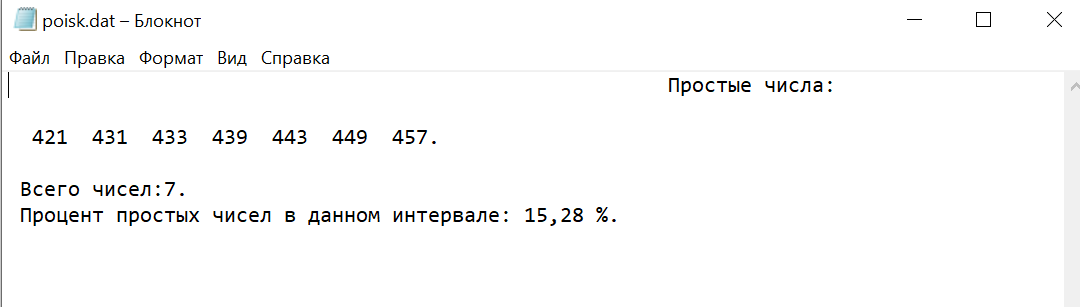


Рисунок 1.3 – Результат поиска простых чисел в заданном интервале

Чтобы найти все простые числа из промежутка используя «решето Эратосфена» надо воспользоваться свойством 3 простых чисел и вычислить √457 ≈ 21,4, т. е. меньше 22. После чего надо записать числа из заданного диапазона (421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457) и удалить последовательно все числа, делящиеся на простые числа от 2 до 22. Такими простыми числами являются: 2, 3, 5, 7, 11, 13, 17,19. После выполнения всех операций в «решете» останутся числа 421, 431, 433, 439, 443, 449, 457.

# **Задание 3**

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

Числа 421 и 457 являются простыми, следовательно их запись будет выглядеть как 421= 421\*1, 457=457\*1.

# **Задание 4**

Проверить, является ли число, состоящее из конкатенации цифр *m* ǀǀ *n*, простым.

Конкатенация чисел 421 и 457 дает число 421457. Результат проверки числа 421457 на простоту приведен на рисунке 1.4.

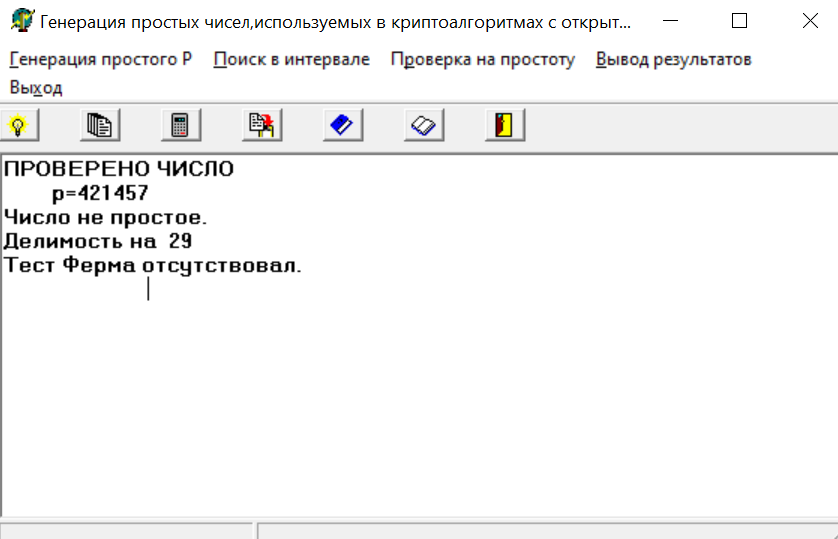


Рисунок 1.4 – Результат проверки числа на простоту

# **Задание 5**

Найти НОД (*m, n*).

421= 421\*1 + 0; 457 = 457 \* 1 +0 наибольший общий делитель равняется 1. НОД(421,457) = 1.

# **2 Основное задание**

Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции: вычислять НОД двух либо трех чисел; выполнять поиск простых чисел. Функция для вычисления НОД двух или трех чисел, представлена в листинге 2.1, функция для выполнения поиска простых чисел в листинге 2.2.

|  |
| --- |
| function NOD(a, b){      while (b !== 0)      {          let temp = b          b = a % b          a = temp      }      return a  }  function NOD3(a, b, c){      return NOD(NOD(a,b), c)  } |

Листинг 2.1 – Функции для вычисления НОД двух или трех чисел

|  |
| --- |
| function findPrimes(a, b) {      let primes = [];      for (let i = Math.max(2, a); i <= b; i++) {          let isPrime = true;          for (let j = 2; j \* j <= i; j++) {              if (i % j === 0) {                  isPrime = false;                  break;              }          }          if (isPrime) primes.push(i);      }      return primes;  } |

Листинг 2.2 – Функции для выполнения поиска простых чисел

С помощью созданного приложения выполнить задания по условиям Задания 1 и 2. Результаты выполнения представлены на рисунке 2.1.

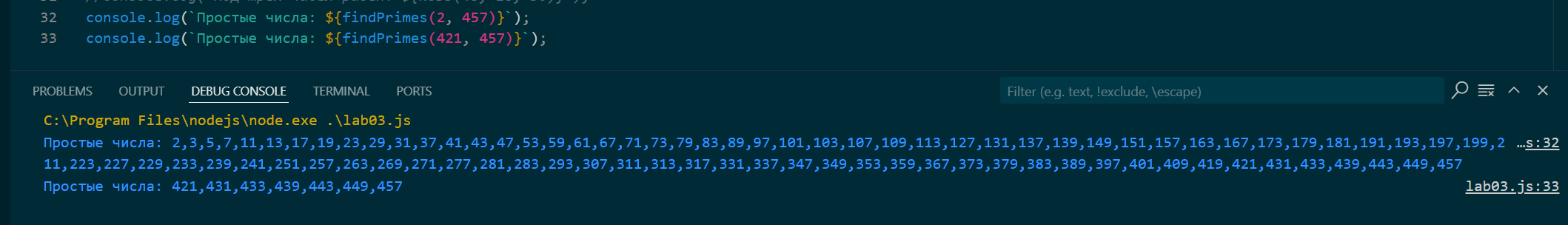


Рисунок 2.1 – Результаты выполнения поиска простых чисел

# **Вывод**

В ходе лабораторной работы удалось не только закрепить теоретические знания высшей арифметики, но и приобрести практические навыки работы с операциями над числами, которые применяются в криптографии. Было освоено решение задач на вычисление НОД, разложение на простые множители, нахождение обратных чисел по модулю и выполнение операций в модульной арифметике. Разработка и тестирование приложения с использованием программного средства L\_PROST подтвердили эффективность автоматизации этих операций и демонстрируют потенциал применения математических методов в решении прикладных криптографических задач.