МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа № 3**

**ОСНОВЫ ТЕОРИИ ЧИСЕЛ**

**И ИХ ИСПОЛЬЗОВАНИЕ В КРИПТОГРАФИИ**

Разработал: Бай И.О.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М.Г.

Минск 2023

**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. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения эксперимента с использованием приложения и результатов эксперимента.

**Практическое задание**

**Вариант 2 *m*=450, *n*=503**

1. Используя L\_PROST, 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*).

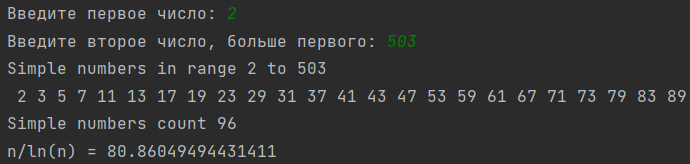


Рис.1 – Реализация поиска простых чисел на интервале

2. Повторить п. 1 для интервала [*m*, *n*].

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

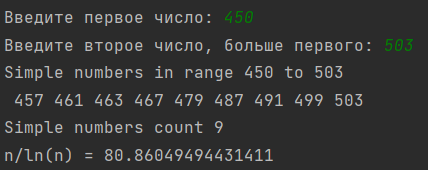


Рис.2 – Реализация поиска простых чисел на интервале

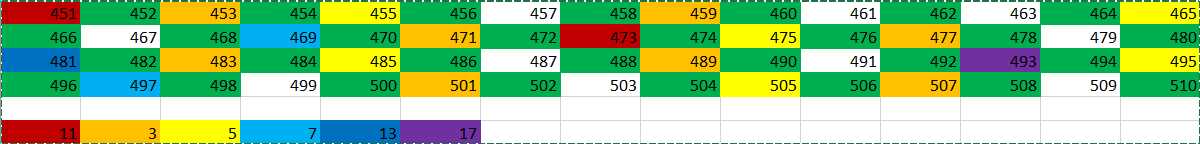


Рис.3 – Решето Эратосфена

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



Рис.4 – Каноническая форма записи числа



Рис.5 – Каноническая форма записи числа

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

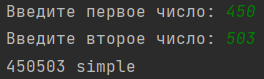


Рис.6 – Определение принадлежности числа к простому

1. Найти НОД (*m*, *n*).

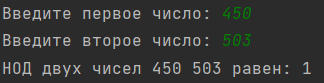


Рис.7 – Нахождение НОД чисел

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

• вычислять НОД двух либо трех чисел;

• выполнять поиск простых чисел.

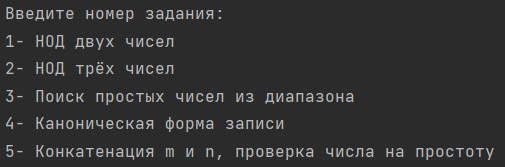


Рис.8 – Реализация интерфейса программы

1. С помощью созданного приложения выполнить задания по условиям п. 1 и 2.

*Реализация функций*

package bay.cripta;  
  
public class Functions {  
 public static int NOD(int x, int y) {  
 while (x != 0 && y != 0) {  
 if (x > y) {  
 x -= y;  
 } else {  
 y -= x;  
 }  
 }  
 return Math.*max*(x, y);  
 }  
  
 public static boolean isSimple(int x) {  
 for (int i = 2; Math.*pow*(i, 2) <= x; i++) {  
 if (x % i == 0) {  
 return false;  
 }  
 }  
 return true;  
 }  
  
 public static void findSimple(int m, int n) {  
 int counter = 0;  
 if (n < m) {  
 System.*out*.println("Wrong range!");  
 }  
 System.*out*.println("Simple numbers in range " + m + " to " + n);  
  
 for (int i = m; i <= n; i++) {  
 if (*isSimple*(i)) {  
 System.*out*.print(" " + i);  
 counter++;  
 }  
 }  
 System.*out*.println();  
 System.*out*.println("Simple numbers count " + counter);  
 }  
  
 public static void canonicalNotation(int x) {  
 String str = "";  
 for (int i = 0; x % 2 == 0; x /= 2) {  
 str += " \* 2";  
 }  
 for (int i = 3; i <= x; ) {  
 if (x % i == 0) {  
 str += " \* " + i;  
 x /= i;  
 if (i == x) {  
 str += " \* " + i;  
 break;  
 }  
 } else {  
 i += 2;  
 }  
 }  
 System.*out*.println(str);  
 }  
}

Листинг 1 – Реализация класса Functions

**Вывод:** в ходе изучения теоретических материалов лабораторной работы и выполнения её практической части были изучены основы теории чисел, используемые в криптографии. Изучены основные свойства простых и составных чисел, взаимно простых чисел, а также признаки делимости чисел. На практике полученные знания были закреплены через создание собственного приложения, реализующего функционал вычисления НОД двух и трёх чисел и получения списка простых чисел в заданном диапазоне.