Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

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

Студент: Яскович М.Э.

ФИТ 3 курс 6 группа

Преподаватель: Сазанова Д.В.

Минск 2023

1. **Описание приложения**

Приложение написано на языке программирования Java и позволяет:

* вычислять НОД двух и трех чисел;
* выполнять поиск простых чисел на промежутке [447; 477];
* находить все простые числа в интервале [2;n];
* сравнивать это число с n/ln(n);
* находить обратное число по модулю.

1. **Методика выполнения поставленных задач**

Для нахождения НОД двух в данном приложении используется алгоритм Евклида. Описание функции приводится на рисунке 2.1.

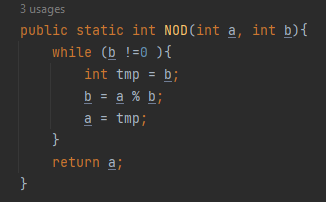


Рисунок 2.1 – Автоматизированный  
 алгоритм Евклида

Для нахождения НОД 3 и более чисел вызывается функция приведенная выше сначала для двух чисел, а затем для третьего числа и НОД первых двух чисел.

Для поиска простых чисел на заданном промежутке используется Решето Эратосфена. Передача границ искомого промежутка осуществляется с консоли. Все целые числа на промежутке записываются в массив, после чего каждый его элемент проверяется на делимость на последовательность простых чисел, и, если остаток равен нулю, удаляется из массива. Описание функции, реализующей данный алгоритм, приведено на рисунке 2.2.

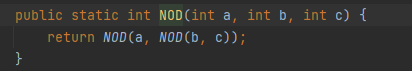


Рисунок 2.3 – Автоматизированное решето Эратосфена

Помимо этого, в приложении реализована функция для нахождения обратного по модулю числа. Использован расширенный алгоритм Евклида, содержимое функции представлено на рисунке 2.4.

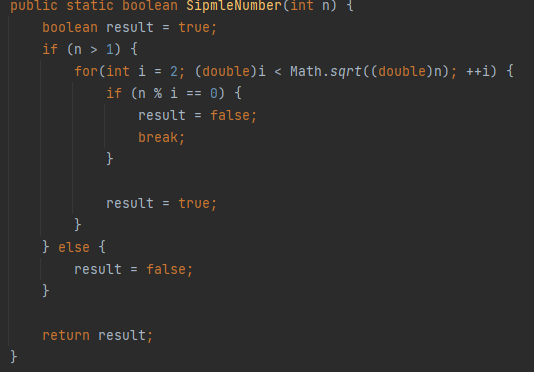
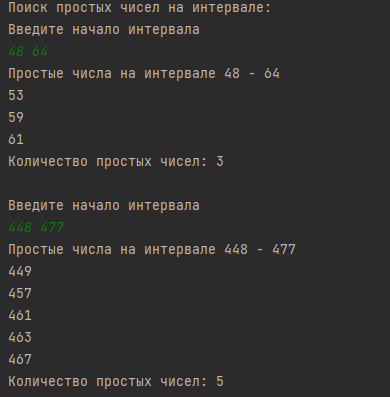
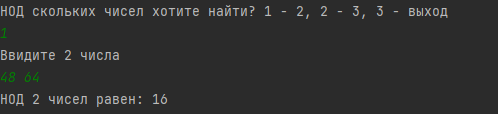
****

Рис. 2.4 – Расширенный алгоритм Евклида

Результат выполнения всех описанных ранее функций выводится на консоль, содержимое которой представлено на рисунке 2.5.





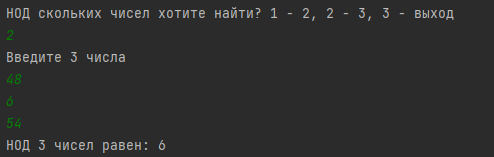


Рисунок 2.5 – Результат выполнения функций

**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.