МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность Информационные системы и технологии

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №12 НА ТЕМУ:**

ОСНОВЫ ТЕОРИИ ЧИСЕЛ И ИХ ИСПОЛЬЗОВАНИЕ В КРИПТОГРАФИИ

Выполнил студент 3 курса 1 группы

Кашперко Василиса Сергеевна

Минск 2022

**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. Разработать приложение для реализации указанных преподавателем операций с числами.

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

**Теоретические сведения**

Для нахождения всех простых чисел не больше заданного числа n в соответствии с «решетом Эратосфена» нужно выполнить следующие шаги:

1. выписать подряд все целые числа от двух (либо от m) до n (2, 3, 4, …, n). Пусть некоторая переменная (напрмер, s) изначально равна 2 – первому простому числу;
2. удалить из списка числа от 2s до n, считая шагами по s (это будут числа, кратные s: 2s, 3s, 4s, …);
3. найти первое из оставшихся чисел в списке, большее чем s, и присвоить значению переменной s это число;
4. повторять шаги 2 и 3, пока возможно.

Наибольшее целое число, которое делит без остатка числа a и b, называется наибольшим общим делителем этих чисел – НОД (a, b). Простым и эффективным средством вычисления НОД (a, b) является алгоритм Евклида.

Чтобы найти НОД нескольких чисел (например, a, b, c), достаточно найти НОД двух чисел (например, НОД (a, b) = d), потом НОД полученного (НОД (a, b)) и следующего числа (НОД (c, d)), и т. д. Используется цепочка вычислений двумя исходными (начальными) числами а и b:

При i = 0 в выражении аi и bi соответствуют как раз числам а и b. Последний ненулевой остаток (ri, i ≥ 0) соответствует НОД (a, b).

Таким образом, чтобы вычислить НОД k чисел, нужно последовательно вычислить (k – 1) НОД. Последнее вычисление дает искомый результат.

**Практическая часть**

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

• вычислять НОД двух либо трех чисел;

• выполнять поиск простых чисел.

Выполнение программы изображено на рисунках 1, 2, 3, 4 и 5.

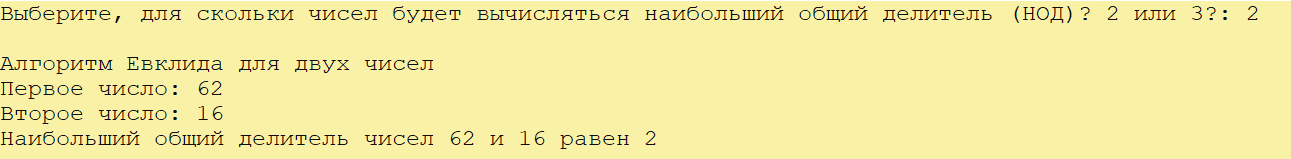


Рисунок 1 – Вычисление НОД для двух чисел

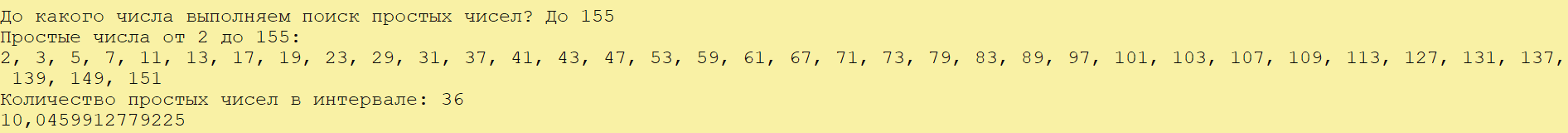


Рисунок 2 – Поиск простых чисел в интервале

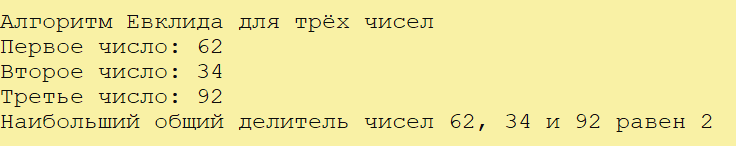


Рисунок 3 – Вычисление НОД для трех чисел

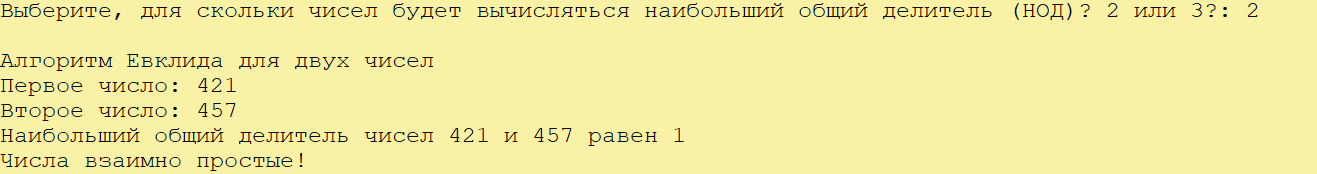


Рисунок 4 – Вычисление НОД для пары чисел в соответствии с вариантом

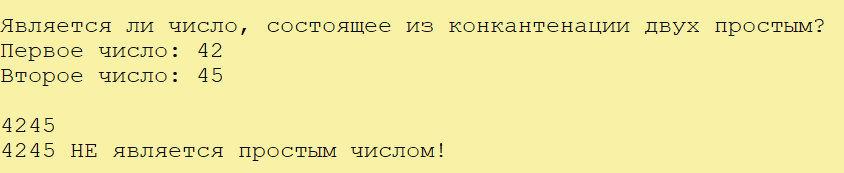


Рисунок 5 – Определение, является ли число, состоящее из конкатенации двух чисел простым числом

**Вывод:** в ходе лабораторной работы были применены практические навыки выполнения операций с числами для решения задач в области криптографии и разработка приложений для автоматизации этих операций. Закреплены теоретические знания по высшей арифметике. С помощью разработанного приложения были выполнены задания по условиям п.1 и 2 методического пособия.