Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**«Отчёт по лабораторной работе №3»**

“ ОСНОВЫ ТЕОРИИ ЧИСЕЛ

И ИХ ИСПОЛЬЗОВАНИЕ В КРИПТОГРАФИИ ”

**Выполнила:** студентка 3 курса

4 группы специальности ПОИТ

Мамаева Диана Александровна

**Проверил:** преподаватель

Капыток Дария Владимировна

Минск 2023

**Теоретические сведенья**

В основе современной криптографии лежит теория чисел.  
Теория чисел, или высшая арифметика, – раздел математики,  
изучающий натуральные числа и иные похожие величины. В зависимости от используемых методов в теории чисел рассматривают  
несколько направлений. Нас будут интересовать вопросы делимости целых чисел, вычисления наибольшего общего делителя (НОД),  
разложение числа на простые множители, малая теорема Ферма́,  
теорема Эйлера, элементы теории вычетов.

**Практическое 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.  
7. С помощью созданного приложения выполнить задания  
по условиям п. 1 и 2.  
8. Результаты выполнения работы оформить в виде отчета  
по установленным правилам.  
Таблица 1.2  
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 |

**Реализация**

Код написан на языке C#

На рисунке 1.1 представлен код реализации нахождения НОД(a,b) и НОД (a,b,c)

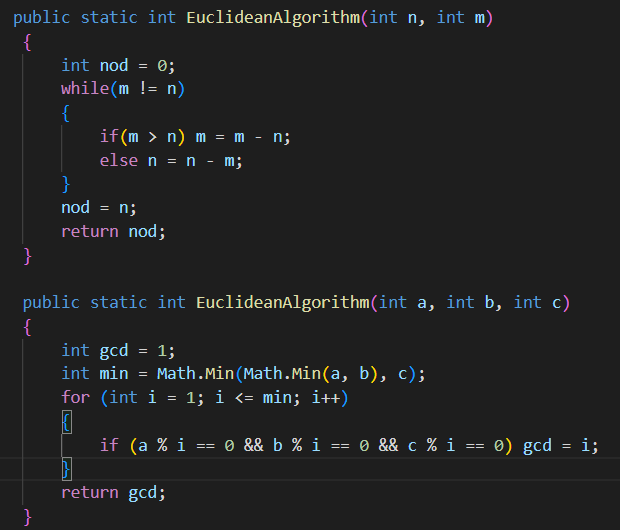


Рис. 1.1 реализация нахождения НОД(a,b,c) и НОД(a,b)

Для поиска простых чисел, была написана специальная функция. Код данной функии представлена на рисунке 1.2

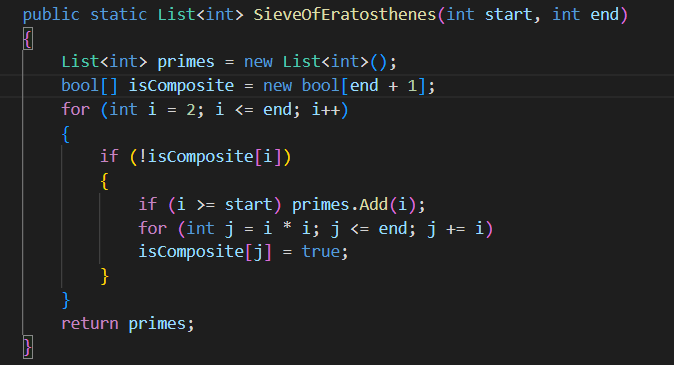


Рис. 1.2 реализация SieveOfEratosthenes