Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Лабораторная работа № 3**

« Основы теории чисел и их использование в криптографии»

Выполнил:

Студент: Шулаков А.А.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М.Г.

**Цель**: 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.

# **Теоретические сведения**

***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.

Множество всех целых чисел (обозначим буквой *Z*) есть набор всех ***действительных чисел*** без дробной части: {..., –3, –2, –1, 0, 1, 2, 3, ...}. Основы теории чисел и их использование в криптографии

***Натуральные числа*** являются подмножеством целых чисел и образуют множество *N*: {1, 2, 3, ...}.

***Делимость*** – одно из основных понятий теории чисел. Если для некоторого целого числа a и натурального числа *b* существует целое число *q*, при котором *bq = a*, то говорят, что число a делится на *b*. В этом случае *b* называется делителем числа *a*, а a называется кратным числу *b*.

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 (например, *s*) изначально равна 2 – первому простому числу;

2) удалить из списка числа от 2*s* до *n*, считая шагами по *s* (это будут числа, кратные *s*: 2*s*, 3*s*, 4*s*, …);

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.

**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 в заданном интервале.

Наибольшее целое число, которое делит без остатка числа *a* и *b* называется наибольшим общим делителем этих чисел, НОД (*m*, *n*).

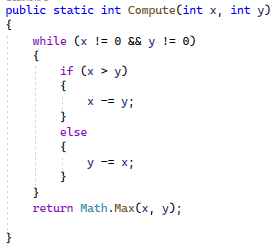


Рисунок 1 — функции вычисления НОД двух чисел на языке C#.

Результат выполнения функции при значениях первого и второго чисел 230 и 432 соответственно представлен на рисунке 2.



Рисунок 2 — результат функции Compute со значениями 230 и 432

Простое число – это натуральное число, единственными делителями которого являются только оно само и единица.

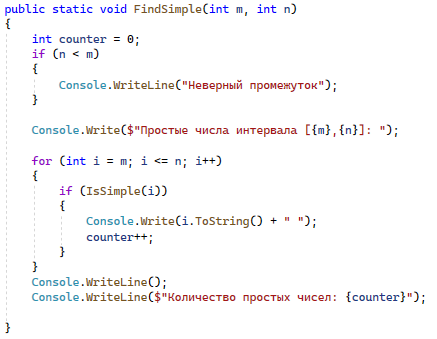


Рисунок 3 — функции нахождения простых чисел в заданном интервале

Для того чтобы определить, является ли число простым была разработана функция IsSimple.

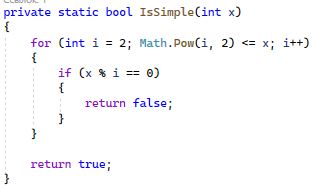


Рисунок 4 — реализация функции IsSimple

Для разбиения числа в виде произведения простых множителей была разработана функция TrialDivision

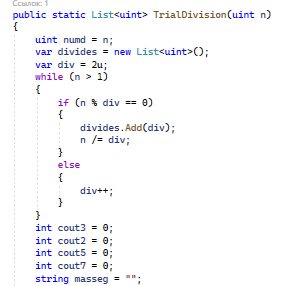


Рисунок 5 — реализация функции TrialDivision

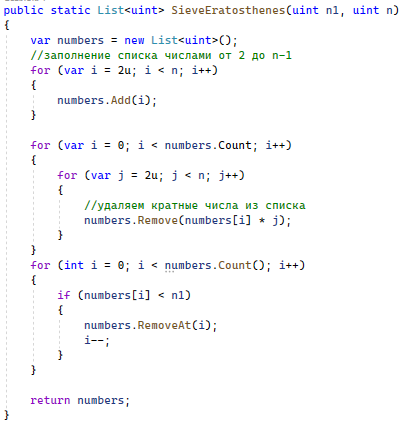


Рисунок 6 — реализация алгоритма «решето Эратосфена»

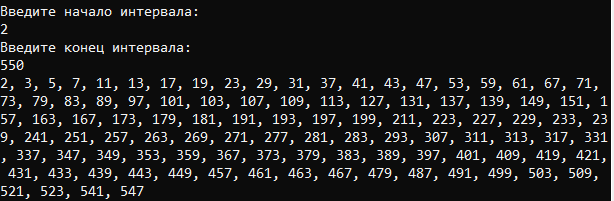


Рисунок 7 — демонстрация работы алгоритма «решето Эратосфена» для интервала от 2 до 550

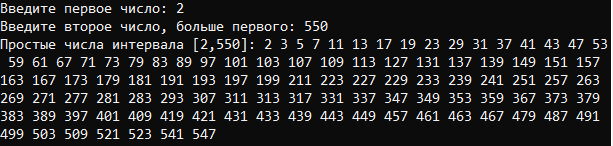


Рисунок 8 — демонстрация работы алгоритма для вычисления простых чисел из интервала от 2 до 550

Решето Эратосфена от 1 до 15:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 |

8- количество простых чисел до 15

Все простые числа до 20: 2, 3, 5, 7, 11, 13.

Зелёные – простые числа.

Красные – составные числа.

**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.