Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы теории чисел и их использование в криптографии

Студент: Голодок А. Ю.

ФИТ 3 курс 4 группа

Преподаватель: Сазонова Д. В.

Минск 2024

1. **Вычисление наибольшего общего делителя**

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

Для нахождения НОД трёх чисел достаточно в качестве одного из параметров указать вызов функции нахождения НОД. Таким образом получен НОД трёх чисел.

Для вычисления наибольшего общего делителя двух и трех чисел реализована следующая функция, представленная на рисунке 1.1:

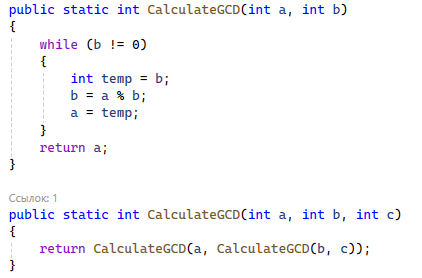


Рисунок 1.1 – Функция нахождения НОД двух и трех чисел

Вывод данной функции, а также функции нахождения НОД (*m, n*), где *m* = 401, *n* = 367, представлен на рисунке 1.2.





Рисунок 1.2 – Вывод НОД двух и трех чисел

1. **Поиск простых чисел**

Для нахождения всех простых чисел не больше заданного числа *n* сначала происходит проверка. Число должно быть больше единицы, равно двум или трем, и не делится без остатка ни на одно другое число. Функция представлена на рисунке 2.1.

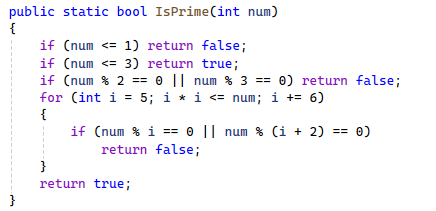


Рисунок 2.1 – Функция поиска простых чисел

Функция для вывода всех простых чисел в диапазоне от m до n представлена на рисунке 2.2.

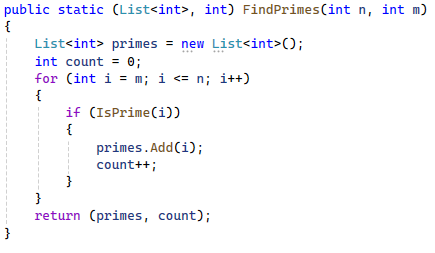


Рисунок 2.1 – Функция отображения простых чисел

Вывод данных функций для поиска простых чисел в интервалах [2, *n*] и [*m*, *n*], а также количество простых чисел в этих диапазонах и значение *n* / ln(*n*) представлены на рисунке 2.3.

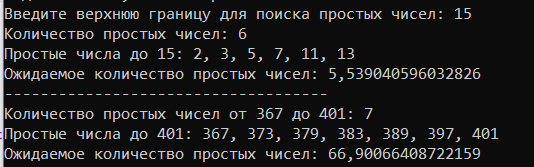


Рисунок 2.3 – Вывод функции поиска простых чисел

1. **Каноническая форма записи числа**

Любое число *n* можно представить в следующем виде, называемое канонической формой записи числа:

 (1.1)

где *p1*, *p2*,…, *pn* – разные простые множители числа, *a1*, *a2*, …, *an* – степени данных простых множителей. Также данные множители можно записывать подряд, по возрастанию, без использования степеней.

Для реализации представления числа в канонической форме реализована следующая функция, представленная на рисунке 3.1.

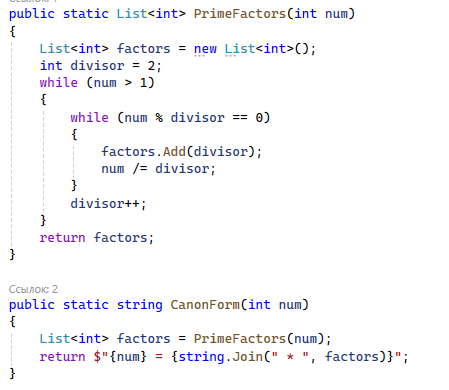


Рисунок 3.1 – Функция представления числа в канонической форме

Функция принимает целое число и ищет его простые множители. Она использует метод деления на простые числа, начиная с 2 и увеличивая делитель до тех пор, пока число не будет разделено на все простые множители. Каждый найденный простой множитель добавляется в список, который возвращается в конце выполнения функции. Этот список содержит все простые множители числа. Вывод данной функции представлен на рисунке 3.2.



Рисунок 3.2 – Вывод канонической формы числа

1. **Конкатенация чисел**

Для выполнения задания проверки на простоту числа, состоящего из конкатенации цифр, из которых состоят числа *m* и *n*, реализована следующая функция, представленная на рисунке 4.2.

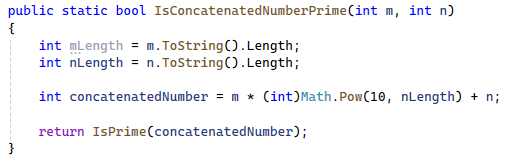


Рисунок 4.2 – Функция конкатенации двух чисел

Далее, необходимо вызвать метод проверки числа на простоту, передав в параметры возвращаемое значение функции конкатенации чисел. Вывод данной функции представлен на рисунке 4.3.



Рисунок 4.3 – Вывод функции проверки на простоту конкатенации чисел

Вывод: в ходе выполнения лабораторной работы были приобретены практические навыки выполнения операций с числами, необходимые для решения задач в области криптографии. Также было разработано приложение, позволяющее автоматизировать данные операции.