Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы теории чисел и их использование в криптографии

Студент: Валдайцев А. Д.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М. Г.

Минск 2023

# Вычисление наибольшего общего делителя

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

Наибольший общий делитель можно найти с помощью алгоритма Евклида, который заключается в том, чтобы от наибольшего числа из двух отнимать наименьшее, пока одно из них не станет равно нулю, а после вернуть наибольшее из двух число.

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

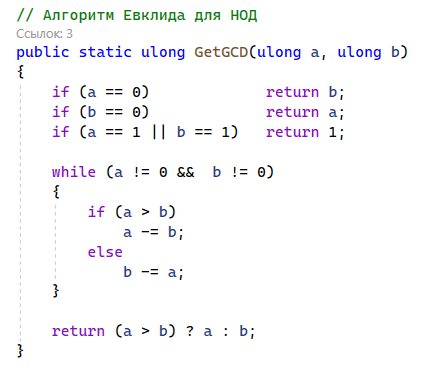


Рисунок 1.1 – функция нахождения НОД двух чисел

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 так далее.

Следовательно, для нахождения НОД трёх чисел достаточно в качестве одного из параметров указать вызов функции нахождения НОД. Таким образом получен НОД трёх чисел. Вывод данной функции, а также функции нахождения НОД (*m, n*), где *m* = 421, *n* = 457, представлен на рисунке 1.2.

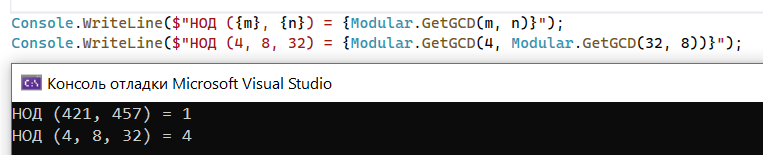


Рисунок 1.2 – вывод НОД двух и трех чисел

# Поиск простых чисел

Для нахождения всех простых чисел не больше заданного числа n используется алгоритм, называемый «решетом Эратосфена». В соответствии с этим алгоритмом нужно выполнить следующие шаги:

1. выписать подряд все целые числа от двух (либо от *m*) до n (2, …, *n*). Пусть некоторая переменная (например, *s*) изначально равна 2, то есть 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.

Для реализации данного алгоритма созданы следующие функции, представленные на рисунке 2.1:

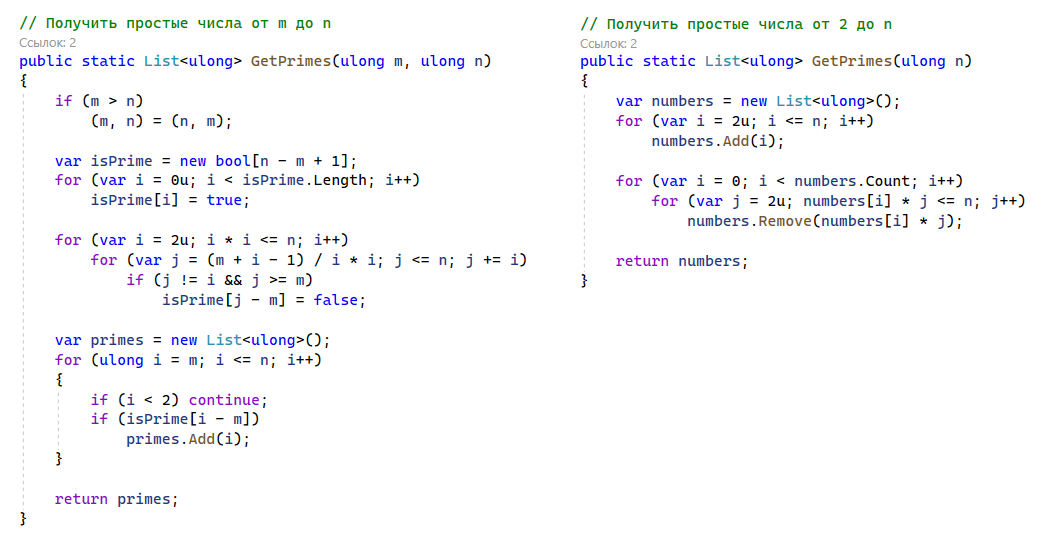


Рисунок 2.1 – функция поиска простых чисел

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 2.2.

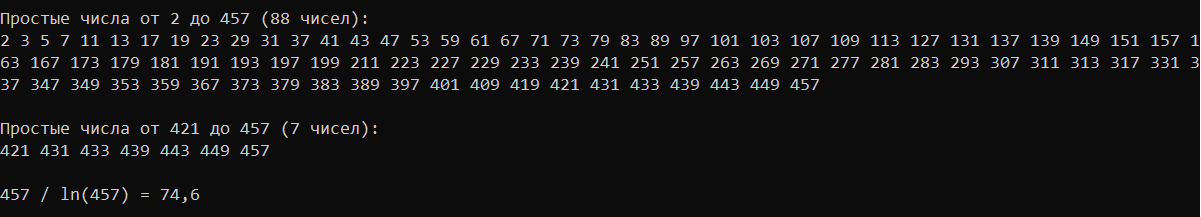


Рисунок 2.2 – вывод функции поиска простых чисел

Для проверки полученных значений можно воспользоваться ручным вычислением решета Эратосфена. На рисунке 2.3 изображено вручную высчитанное решето Эратосфена, где красным выделены вычеркнутые в ходе алгоритма числа, а зелёным – оставшиеся простые числа в диапазоне [*m*, *n*].

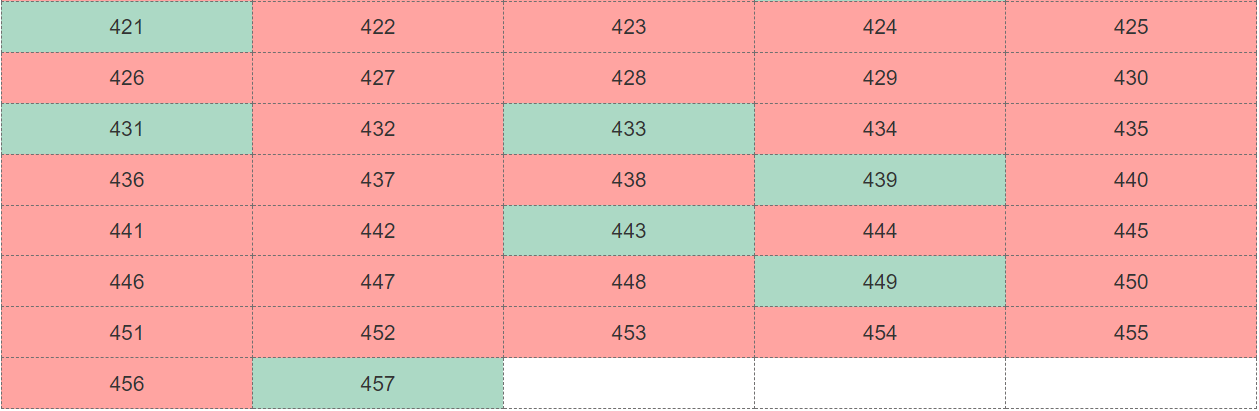


Рисунок 2.3 – решето Эратосфена в диапазоне [*m*, *n*]

Аналогично высчитывается решето Эратосфена для чисел в диапазоне [2, *n*], равное 88, что отражено на рисунке 2.4.

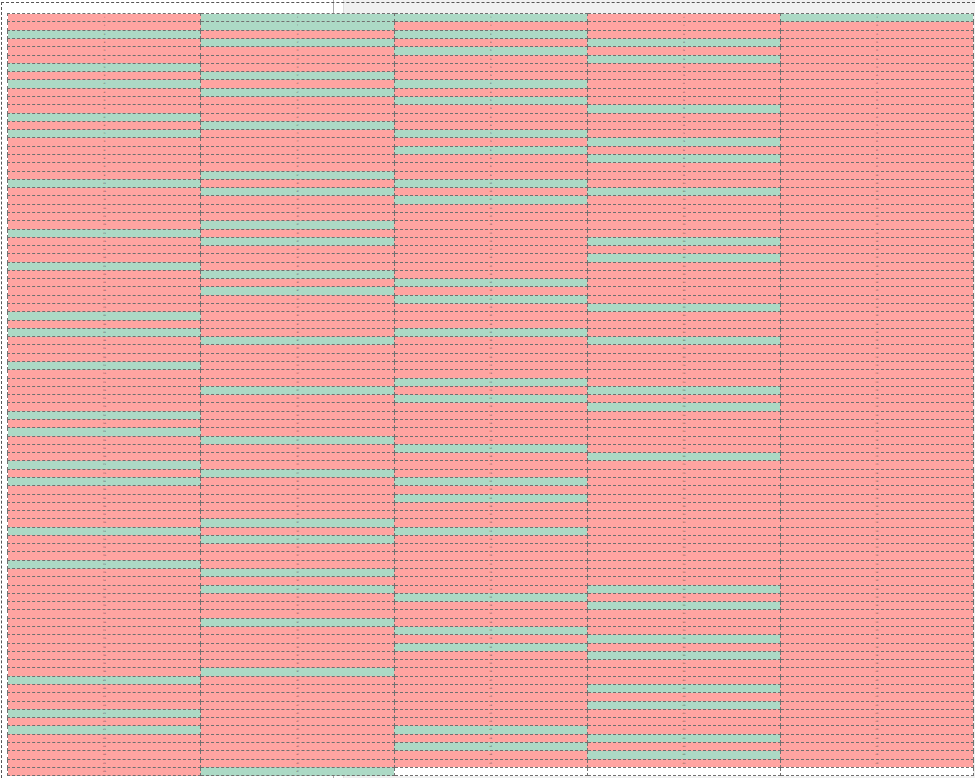


Рисунок 2.4 – решето Эратосфена в диапазоне [2, *n*]