Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

Основы теории чисел и их использование в криптографии

Выполнил:

студент 3 курса 4 группы

специальности ПОИТ

Матюх А.А.

Минск 2020

1. **Теоретические сведения**

Свойство 1. Любое составное число представляется уникальным образом в виде произведения простых чисел; иначе еще говорят, что разложение числа на простые множители однозначно.

Основная теорема арифметики. Всякое натуральное число n, кроме 1, можно представить как произведение простых множителей

Свойство 2. Простых чисел бесконечно много, причем существует примерно n/ln(n) простых чисел, меньших числа n.

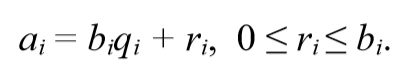
Свойство 3. Наименьший простой делитель составного числа n не превышает √n, поэтому для проверки простоты числа достаточно проверить его делимость на 2 и на все нечетные (а еще лучше простые) числа, не превосходящие √n; как видим, данное свойство коррелирует со свойством 1 собственного делителя.

«Решето Эратосфена». Его суть в последовательном исключении из списка целых чисел от 1 до n чисел (или из сокращенного диапазона, например, от m до n, 1<m≤n), кратных 2, 3, 5 и другим простым числам, уже найденным «решетом».

Понятие делимости чисел является одним из важных в теории чисел. С этим понятием, а также с его производным – общим делителем связаны другие важнейшие (в частности, для криптографии) понятия: наибольшего общего делителя (НОД) и взаимно простых чисел.

Определение 9. 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 метод или алгоритм Евклида. В основе алгоритма лежит цепочка вычислений двумя исходными (начальными) числами: а и b:



Определение 10. Взаимно простыми являются целые числа, наибольший общий делитель которых равен 1.

Теорема 1. Целые числа a и b взаимно просты тогда и только тогда, когда существуют такие целые u и v, что выполняется равенство аu + bv = 1.

Теорема 2. Если НОД (a, b) = d , то справедливо следующее соотношение (соотношение Безу): аu + bv = d.

1. **Практическая часть**

В данной лабораторной работе необходимо разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:

• вычислять НОД двух либо трех чисел;

• выполнять поиск простых чисел.

Пример нахождения количества простых чисел:

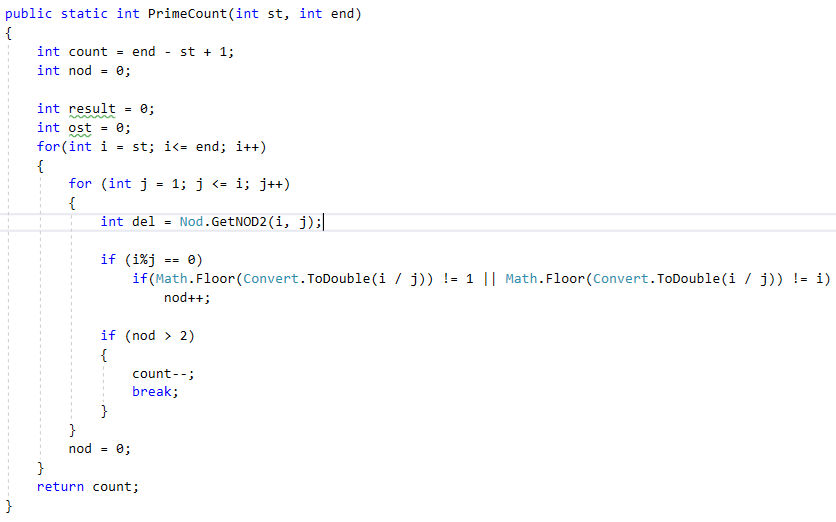


Рисунок 2.1 – Пример нахождения количества простых чисел

Пример нахождения НОД 2 и 3 значений:

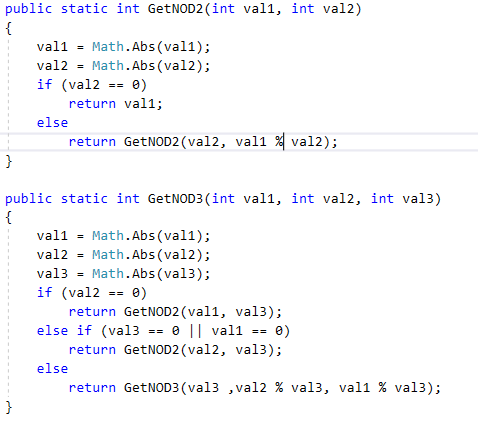


Рисунок 2.2 – Пример нахождения НОД 2 и 3 значений

**Вывод**

В данной лабораторной работе я закрепил теоретические знания по теории чисел. А также, разработал приложение для нахождения НОД и простых чисел.