МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**«Отчет к лабораторной работе №3 Основы теории чисел и их использование в криптографии»**

Студент:

Септилко Анастасия Антоновна

Преподаватель:

Блинова Евгения Александровна

Минск 2020

1. **Описание приложения**

Приложение написано на языке программирования C# и позволяет провести расчет НОД двух либо трех чисел, а также найти все простые числа в заданном промежутке и рассчитать обратное по модулю число, применив расширенный алгоритм Евклида.

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 наибольшегообщего делителя (НОД), разложение числа на простые множители, малаятеорема Ферма́ , теорема Эйлера, элементы теории вычетов.

1. **Описание выполнения заданий и результат выполнения**
2. Найти все простые числа в интервале [2, n]. Значение n соответствует варианту из таблицы 1.1 в методическом пособии, указанному преподавателем. Подсчитать количество простых чисел в указанном интервале. Сравнить это число с n/ln(n).
3. Повторить п.1 для интервала [m, n]. Сравнить полученные результаты с «ручными» вычислениями, используя «решето Эратосфена».
4. Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:

• вычислять НОД двух либо трех чисел;

• выполнять поиск простых чисел.

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

В моем случае m=667 n =703. Пример функции высчитывающая НОД приведена на рисунке 1.1.

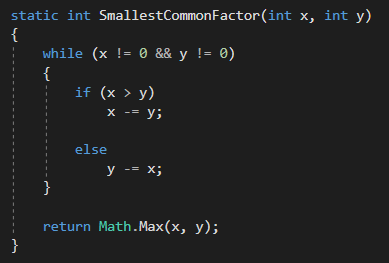


Рисунок 1.1

Результат выполнения функции показан на рисунке 1.2.

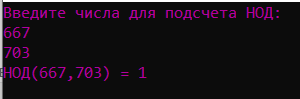


Рисунок 1.2

Подсчет простых чисел в интервале от 2 до 703 реализован с помощью функции SimplesInInterval (рисунок 1.3).

Если число не имеет делителей, кроме самого себя и единицы, то оно  
называется простым, а если у числа есть еще делители, то составным.  
Натуральное число n называется простым, если n > 1 и не  
имеет положительных делителей, отличных от 1 и n.  
Простое число не делится без остатка ни на одно другое число.

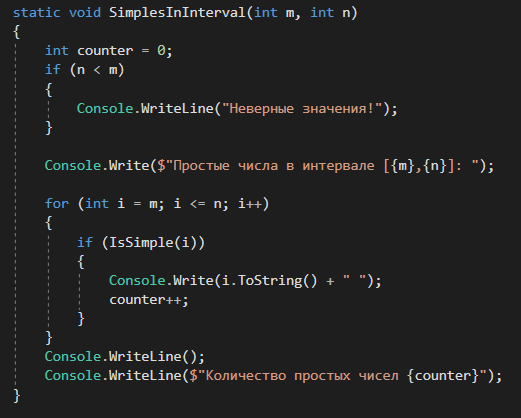


Рисунок 1.3

Для того чтобы определить, является ли число простым была разработана функция IsSimple(int х). На рисунке 1.4 показана.

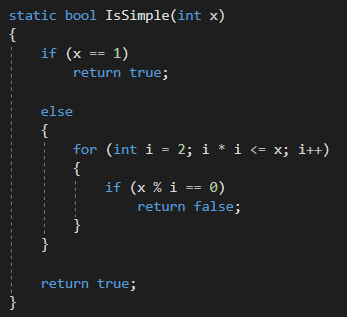


Рисунок 1.4

Результат выполнения функции показан на рисунке 1.5.

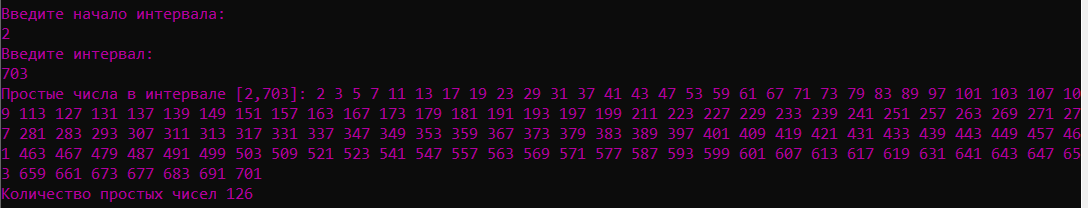
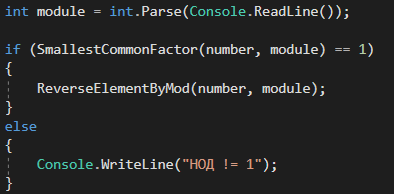


Рисунок 1.5

Так же по заданию требовалось разработать функцию вычисления обратного по модулю числа, т. е. разработать реализацию расширенного алгоритма Евклида. Расчеты в данной функции производятся с введенными пользователем с консоли значениями (рисунок 1.6).



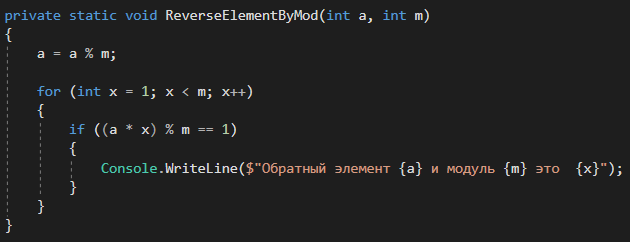


Рисунок 1.6

Результат выполнения функции показан на рисунке 1.7.

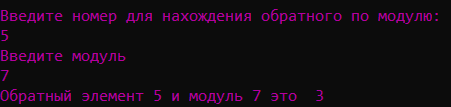


Рисунок 1.7

**Вывод**

Приобрела практические навыки выполнения операций с числами для решения задач в области криптографии и разработала приложение для автоматизации этих операций.

Удостоверилась что разработанное приложение работает корректно и правильно.

**ОТВЕТЫ НА ВОПРОСЫ ДЛЯ КОНТРОЛЯ И САМОКОНТРОЛЯ**

1. **Дать определение понятий: целое число, натуральное число, делимость чисел, собственный делитель, НОД.**

Целое число –Множество всех целых чисел (обозначим буквой Z) есть  
набор всех действительных чисел без дробной части: {..., -3, -2, -1, 0, 1, 2, 3,...}.

Множество всех целых чисел (обозначим буквой Z) есть  
набор всех действительных чисел без дробной части: {..., -3, -2, -1, 0, 1, 2, 3,  
...}.Делимость – одно из основных понятий теории чисел.  
Если для некоторого целого числа a и натурального числа b существует целое  
число q, такое, что bq=a, то говорят, что число a делится на b. В этом случае bназывается делителем числа a, а a называется кратным числа b.

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

1. **Сформулировать основную теорему арифметики. Представить примеры ее применения.**

Всякое натуральное число n, кроме 1,  
можно представить как произведение простых множителей:  
n = p1 · p2 · p3 · ... · pz, z > 1. (1.1)  
Пример 3. Целое число 1554985071 = 3·3·4463 ·38713 – произведение четырех простых чисел, два из которых совпадают.  
Пример 4. Целое число 39616304 = 2·13·7·2·23·13·2·13·2·7 =  
= 2·2·2·2·7·7·13·13·13·23.

1. **Пояснить сущность проблемы факторизации и ее связь с прикладной криптографией**

Факторизацией [натурального числа](https://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D1%82%D1%83%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE) называется его разложение в произведение [простых множителей](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B9_%D0%BC%D0%BD%D0%BE%D0%B6%D0%B8%D1%82%D0%B5%D0%BB%D1%8C). Существование и единственность (с точностью до порядка следования множителей) такого разложения следует из [основной теоремы арифметики](https://ru.wikipedia.org/wiki/%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D0%BD%D0%B0%D1%8F_%D1%82%D0%B5%D0%BE%D1%80%D0%B5%D0%BC%D0%B0_%D0%B0%D1%80%D0%B8%D1%84%D0%BC%D0%B5%D1%82%D0%B8%D0%BA%D0%B8).

В отличие от задачи [распознавания простоты](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%81%D1%82_%D0%BF%D1%80%D0%BE%D1%81%D1%82%D0%BE%D1%82%D1%8B) числа, [факторизация](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%BA%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F) предположительно является [вычислительно сложной](https://ru.wikipedia.org/wiki/%D0%92%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%BB%D0%BE%D0%B6%D0%BD%D0%BE%D1%81%D1%82%D1%8C) задачей. В настоящее время неизвестно, существует ли [эффективный](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B0%D1%81%D1%81_P) не [квантовый алгоритм](https://ru.wikipedia.org/wiki/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D1%8B%D0%B9_%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC) факторизации целых чисел. Однако доказательства того, что не существует решения этой задачи за полиномиальное время, также нет.

Предположение о том, что для больших чисел задача факторизации является вычислительно сложной, лежит в основе широко используемых алгоритмов (например, [RSA](https://ru.wikipedia.org/wiki/RSA)). Множество областей математики и информатики находят применение в решении этой задачи.

1. НОД(333,100)=1, НОД(56,200)=8, НОД(99,200)=1, НОД(61,987)=1, НОД(123,456)=3, НОД(21,43,342)=1, НОД(57,31,200)=1, НОД(42,11,98)=1,
2. **Записать каноническое разложение чисел: 2770, 3780, 6224.**

2770 = 2 · 5 · 277

3780 = 2 · 2 · 3 · 3 · 3 · 5 · 7 = 22 · 33 · 5 · 7

6224 = 2 · 2 · 2 · 2 · 389 = 24 · 389

1. **Записать соотношение Безу. Показать пример его практического использования**
2. **Если НОД (a, b) = d , то справедливо следующее соотношение  
   (соотношение Безу):**аu + bv = d
3. **Подсчитать число взаимно простых чисел с числами 2770, 3780, 6224** : 1104, 864, 3104
4. **Сформулировать малую теорему Ферма. Показать примеры ее практического применения**

Малая теорема Ферма. Если n – простое число, а число а не кратно n, то справедливо:an ≡ 1 mod n. В соответствии с обобщением Эйлера приведенной теоремы, если НОД (а,n) =1, то справедливо:aφ(n) mod n ≡ 1.   
Последнее выражение можно переписать в следующем виде:  
а-1 mod n ≡ aφ(n)-1 mod n.

1. **Пояснить порядок операций на основе расширенного алгоритма Евклида**

Находим НОД (7,40) – прямая прогонка (алгоритм Евклида):  
40 = 7·5 + 5,  
7 = 5·1 + 2,  
5 = 2·2 + 1, т. е. НОД (7,40) = 1.  
  
1=5–2·2=5–2(7–5·1)=5·3+7(-2)=(40–7·5)3+7(-2) = 40·3+7(-17) = kn + ху=1(mod  
n), или 7(-17) = 7y, так как -17 mod 40 = 23, то у=23: число 23 является обратным  
числу 7 по модулю 40.

Таким образом, сначала представляем первое число через второе плюс остаток, зачем представляем второе число через остаток предыдущего и подобное повторяем до получения остатка 1. Затем идем от последнего выражения до первого, выражая значения через разность, результатом которой будет 1, проводим данное действие пока не получим уравнение вида xy + kn =1

1. **Найти числа обратные к а по модулю n: a = 41, n = 143; a = 13, n = 71: 7, 11**