Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Дисциплина «Защита информации и надежность информационных систем»

**Лабораторная работа №1**

**Тема «ОСНОВЫ ТЕОРИИ ЧИСЕЛ И ИХ ИСПОЛЬЗОВАНИЕ В КРИПТОГРАФИИ»**

Выполнил:

Студент 4 курса 7 группы ФИТ

Тышкевич Р. А.   
 Проверил:   
 Нистюк О. А.

Минск 2024

**Цель:** Приобретение практических навыков выполнения операций с числами для решения задач в области криптографии и разработка приложений для автоматизации этих операций.

**Задачи:**

1. Закрепить теоретические знания по высшей арифметике.

2. Научиться практически решать задачи с использованием простых и взаимно простых чисел, вычислений по правилам модулярной арифметики и нахождению обратных чисел по модулю.

3. Ознакомиться с особенностями реализации готового программного средства L\_PROST и особенностями выполнения с его помощью операций над простыми числами.

4. Разработать приложение для реализации указанных преподавателем операций с числами.

5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения эксперимента с использованием приложения и результатов эксперимента

**Теоретические сведения**

В основе современной криптографии лежит теория чисел. 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.

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

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

Определение 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. При этом используются следующие обозначения: a ⋮ b – a делится на b, или b | a – b делит a. Из последнего определения следует, что:

• любое натуральное число является делителем нуля; • единица является делителем любого целого числа;

• любое натуральное число является делителем самого себя.

Определение 4. Делитель a называется собственным делителем числа b, если 1 < |a| < |b|, и несобственным – в противном случае. Пример 1. 4 | 20; число 4 делит число 20, так как 20 = 4 · 5. При этом число 4 является собственным делителем числа 20. Свойство 1 собственного делителя: положительный наименьший собственный делитель составного числа n не превосходит √n. Определение 5. Всякое целое число а можно представить с помощью положительного целого числа b равенством вида а = bq + r, 0 ≤ r ≤ b. Число q называется неполным частным, а число r – остатком отделения а на b.

Каждое натуральное число, большее единицы, делится по крайней мере на два числа: на 1 и на само себя. Если число не имеет делителей, кроме самого себя и единицы, то оно называется простым, а если у числа есть еще делители, то составным. Определение 6. 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. Пример 2. Первые 10 простых чисел: 2, 3, 5, 7, 11, 13, 17, 19, 23 и 29. Простыми также являются числа 73, 2521, 2 365 347 734 339. Количество простых чисел бесконечно велико. Перечислим несколько важных свойств простых чисел.

Свойство 1. Любое составное число представляется уникальным образом в виде произведения простых чисел; иначе еще говорят, что разложение числа на простые множители однозначно. Это свойство вытекает из основной теоремы арифметики. Основная теорема арифметики. Всякое натуральное число n, кроме 1, можно представить как произведение простых множителей: n = p1p2p3...pz, z > 1.

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. Из соотношения n = qp натуральных чисел, больших единицы, следует, что либо p, либо q принадлежит отрезку от 2 до √n. Поиск сомножителей числа n может вестись, например, перебором всех простых чисел до √n. Однако если множители – большие простые числа, то на их поиск может потребоваться много времени. Сложность решения задачи разложения больших чисел на простые сомножители, известной как «проблема факторизации», определяет криптостойкость некоторых алгоритмов асимметричной криптографии, в частности алгоритма RSA.

Свойство 4. Любое четное число, большее 2, представимо в виде суммы двух простых чисел, а любое нечетное, большее 5, представимо в виде суммы трех простых чисел.

Свойство 5. Для любого натурального n, большего 1, существует хотя бы одно простое число на интервале от n до 2n.

Понятие делимости чисел (см. определение 3) является одним из важных в теории чисел. С этим понятием, а также с его производным – общим делителем (см. определение 4) 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). Пример 13. Делителями числа a = 24 являются: 1, 2, 4, 6, 8, 12, 24; делителями числа b = 32 являютс: 1, 2, 4, 8, 16, 32. Как видим, НОД (24, 32) = 8. Понятно, что значение НОД можно вычислять для неограниченного ряда чисел. Простым и эффективным средством вычисления НОД (a, b) является алгоритм Евклида (примеры его использования приведены в [3]). В основе алгоритма лежит определение 5. В соответствии с этим определением используется цепочка вычислений двумя исходными (начальными) числами а и b: аi = biqi + ri, 0 ≤ ri ≤ bi. (1.2) При i = 0 в выражении (1.2) аi и bi соответствуют как раз числам а и b. Последний ненулевой остаток (ri, i ≥ 0) соответствует НОД (a, b).

**Практическое задание**

1. Используя L\_PROST, найти все простые числа в интервале [2, n]. Значение n соответствует варианту из табл. 1.2, указанному преподавателем. Подсчитать количество простых чисел в указанном интервале. Сравнить это число с n/ln(n) (см. выше пример 15).

2. Повторить п. 1 для интервала [m, n]. Сравнить полученные результаты с «ручными» вычислениями, используя «решето Эратосфена» (см. примеры 11 и 12).

3. Записать числа m и n в виде произведения простых множителей (форма записи – каноническая).

4. Проверить, является ли число, состоящее из конкатенации цифр m ǀǀ n (табл. 1.2), простым.

5. Найти НОД (m, n).

**Основное задание**

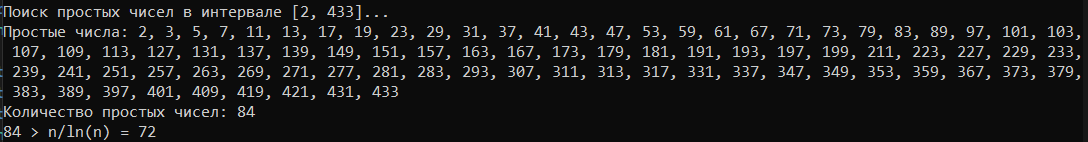
6. Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:

• вычислять НОД двух либо трех чисел;

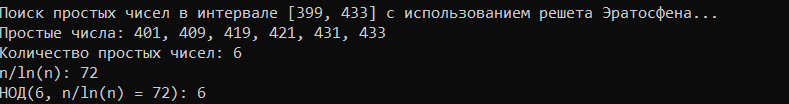
• выполнять поиск простых чисел.

7. С помощью созданного приложения выполнить задания по условиям п. 1 и 2.

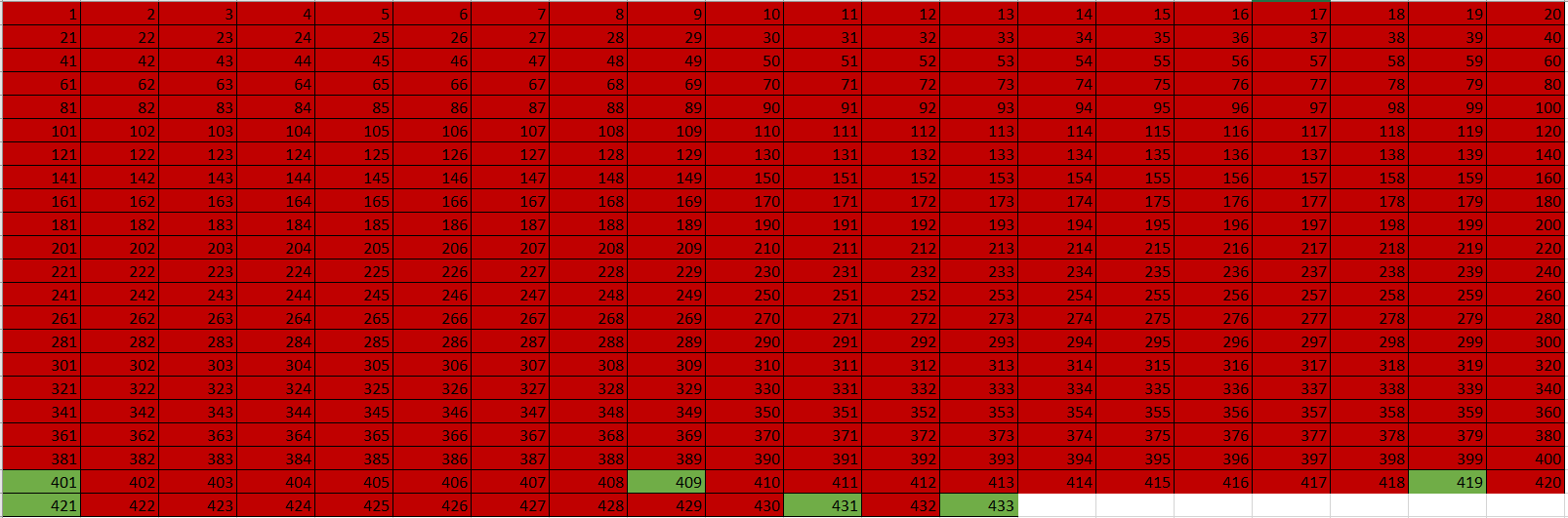
8. Результаты выполнения работы оформить в виде отчета по установленным правилам.



Задание 1



Задание 2



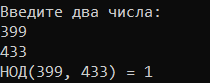
Ручной подсчет для задания 2



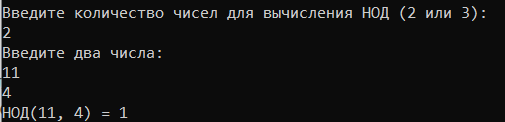
Задание 3

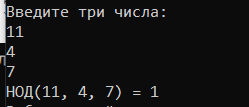


Задание 4



Задание 5





Задание 6

**Вывод:** в результате выполнения лабораторной работы были приобретены практические навыки выполнения операций с числами для решения задач в области криптографии и разработки приложений для автоматизации этих операций.