Министерство образования Республики Беларусь

Учреждение образование

«Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

«Основы теории чисел и их использование в криптографии»

Выполнил:

студент 3 курса 8 группы ФИТ

Ярмолик Николай Сергеевич

Проверил:

Берников В. О.

Минск 2020

**1 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.

Определение 4. Делитель a называется собственным делителем числа b, если 1<|a|

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 от деления 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

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.

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.

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 чем 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.

Определение 7. Натуральное число n называется составным, если n > 1 и имеет, по крайней мере, один положительный делитель, отличный от 1 и n.

Свойство 2 собственного делителя. Положительный наименьший собственный делитель составного числа n есть простое число. Так как простое число не делится ни на какое другое, кроме себя самого, очевидный способ проверки числа n на простоту – разделить n на все числа n1 и проанализировать наличие остатка от деления. Этот способ «в лоб» часто реализуется в компьютерных программах. Однако перебор может оказаться достаточно трудоемким, если на простоту нужно проверить число с количеством цифр в несколько десятков. Существует правила, способные заметно сократить время вычислений

Определение 8. Если два простых числа отличаются на 2, то их называют числами-близнецами. Таких чисел не очень много.

Правило 5. Основано на свойстве делимости на 11. Нужно из суммы всех нечетных цифр числа вычесть сумму всех четных его цифр. Четность и нечетность определяется счетом от младшего разряда. Если получившаяся разность делится на 11, то и анализируемое число тоже на него делится.

Правило 6. Основано на свойстве делимости на 7 и 13. Нужно разбить анализируемое число на тройки цифр, начиная с младших разрядов. Просуммировать числа, стоящие на нечетных позициях, и вычесть из них сумму чисел на четных. Проверить делимость результата на числа 7 и 13.

Например, ими являются 5 и 7, 29 и 31, 149 и 151. Всякое натуральное число n > 1либо является простым числом, либо имеет простой делитель.

Для нахождения всех простых чисел не больше заданного числа n в соответствии с «решетом Эратосфена» нужно выполнить следующие шаги:

1. Выписать подряд все целые числа от двух (либо от m) до n (2, 3, 4, …, n). Пусть некоторая переменная (положим s) изначально равна 2 – первому простому числу.

2. Удалить из списка числа от 2s до n, считая шагами по s (это будут числа кратные s: 2s, 3s, 4s, …).

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.

Определение 9. Наибольшее целое число, которое делит без остатка числа a и b называется наибольшим общим делителем этих чисел, НОД (a, b).

Понятно, что значение НОД можно вычислять для неограниченного ряда чисел. Простым и эффективным средством вычисления НОД (a, b) является метод или алгоритм Евклида

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 т. д.

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.

Понятие «модулярная арифметика» ввел немецкий ученый Гаусс. В этой арифметике мы интересуемся остатком от деления числа а на число n (n – натуральное число и n>1). Если таким остатком является число b, то можно записать: a ≡ b (mod n) или a ≡ b mod n.

Модулярная арифметика так же коммутативна, ассоциативна и дистрибутивна, как и обычная арифметика. В силу этих свойств сравнения можно почленно складывать, вычитать, умножать, возводить в степень (а m mod n ≡ (а mod n) m , если a ≡ b mod n, то a m ≡ b m (mod n);

Малая теорема Ферма. Если n – простое число, а число а не кратно n, то справедливо: a n ≡ 1 mod n.

В соответствии с обобщением Эйлера приведенной теоремы, если НОД (а, n) =1, то справедливо: a φ(n) mod n ≡ 1.

**2 Практическая часть**

В данной лабораторной работе необходимо разработать программу способную вычислять НОД двух либо трех чисел, а также способную выполнять поиск простых чисел в диапазоне.

Расчет НОД для двух произвольных чисел приведен ниже:

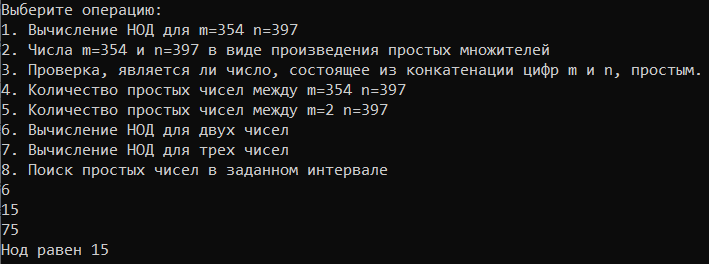


Рисунок 2.1 *–* Расчет НОД для двух произвольных чисел

Далее приведен скриншот расчета НОД для трех произвольных чисел:

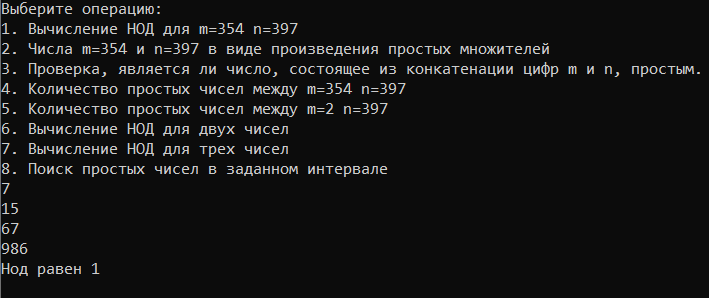


Рисунок 2.2 – Расчет НОД для трех произвольных чисел

Теперь построим гистограмму частоты символов для этого алфавита.

Также необходимо было выполнить дополнительные задания, приведенные в пункте 1 и 2, а именно расчет НОД для чисел m и n, согласно варианту.

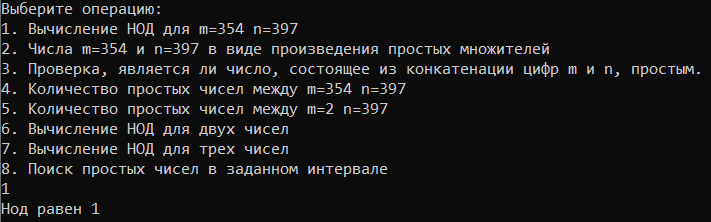


Рисунок 2.3 – Расчет НОД для чисел m и n

Также найти количество простых чисел в диапазоне от n до m, а также от 2 до n, согласно варианту

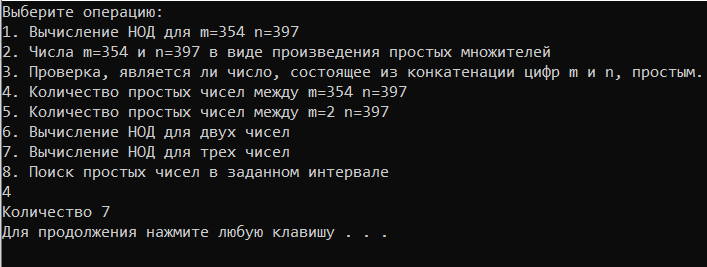


Рисунок 2.4 – Количество простых чисел от n до m

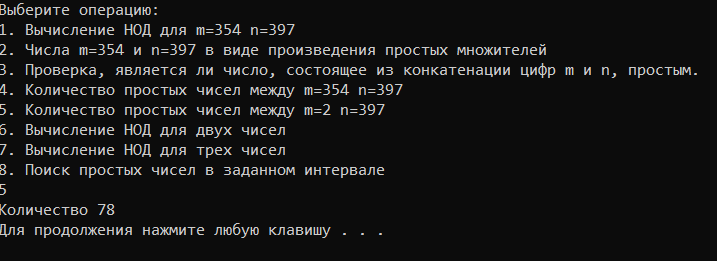


Рисунок 2.5 – Количество простых чисел в диапазоне от 2 до n

Также была реализована возможность разложения чисел m и n на простые множители:

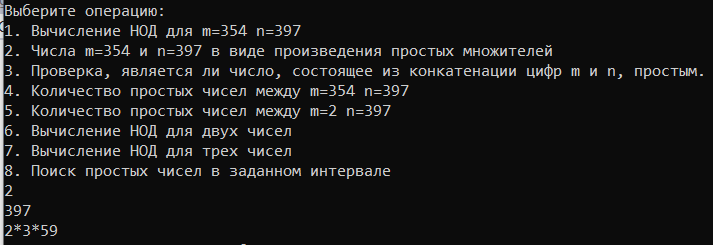


Рисунок 2.6 – Разложение чисел на простые множители

Вывод: В данной лабораторной работе были получены практические навыки расчета НОД для двух и трех чисел, а также нахождение простых чисел в диапазоне с расчетом их количества. Также было реализовано разложение числа на простые множители.