# МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

# Учреждение образования «Белорусский государственный технологический университет»

# 

# Отчёт по лабораторной работе №1

ОСНОВЫ ТЕОРИИ ЧИСЕЛ И ИХ ИСПОЛЬЗОВАНИЕ В КРИПТОГРАФИИ

Выполнил: студент 3 курса специальности ИСиТ Калоша И.В.

Проверила: Копыток Д. В.

Минск 2021

# Основы теории чисел и их использование в криптографии

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

# 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.

. 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.

Если число не имеет делителей, кроме самого себя и единицы, то оно называется простым, а если у числа есть еще делители, то составным.

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

Сложность решения задачи разложения больших чисел на простые сомножители, известной как «проблема факторизации», определяет криптостойкость некоторых алгоритмов асимметричной криптографии, в частности алгоритма RSA.

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

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

# аu + bv = 1. (1.3)

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

# аu + bv = d. (1.4)

Формула (1.4) называется также реализацией «расширенного алгоритма Евклида». Этот алгоритм состоит из двух этапов: собственно алгоритма Евклида и вычислений на основе обратных подстановок или последовательного выражения остатков в каждом из шагов предыдущего этапа с соответствующим приведением подобных на каждом шаге.

# Ход работы

Задание 1. 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).

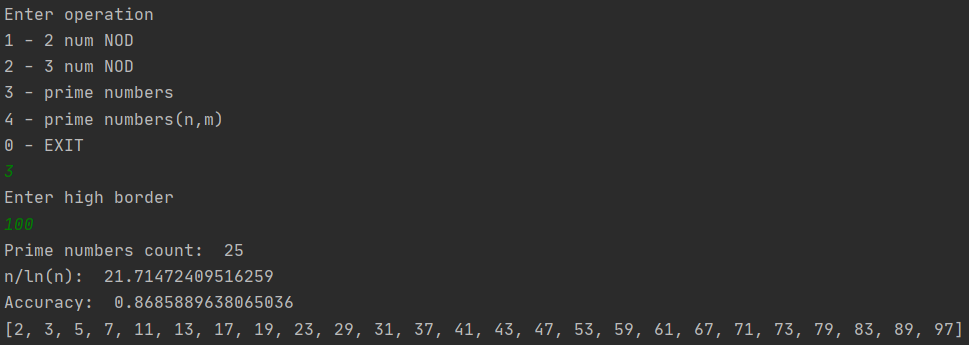


Рисунок 1 – Простые числа [2, n]

Задание 2. Найти все простые числа в интервале [n, m]. Значение n соответствует варианту из табл. 1.2, указанному преподавателем. Подсчитать количество простых чисел в указанном интервале. Сравнить это число с n/ln(n).

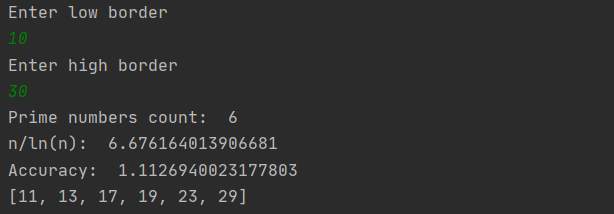


Рисунок 2 – Простые числа [n, m]

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Число** | **Разложение** | **Число** | **Разложение** |
| 499 | 499 | 531 | 3 |
| 1 |  | 177 | 3 |
|  |  | 59 | 59 |
|  |  | 1 |  |

Задание 4. Проверить, является ли число, состоящее из конкатенации цифр m ǀǀ n, простым.

|  |  |
| --- | --- |
| **Число** | **Разложение** |
| 299531 | 47 |
| 6373 | 6373 |
| 1 |  |

Задание 5. Найти НОД (m, n).

НОД(499, 531) = 1, так как 499 простое число.

Код программы для выполнения заданий.

import math

from math import gcd as nod

def count2\_nod(x, y):

return nod(x, y)

def count3\_nod(x, y, z):

x\_y\_nod = count2\_nod(x, y)

return nod(x\_y\_nod, z)

def eratosfen(n):

list = []

k=0

for i in range(2,n+1):

for j in range (2,i):

if i%j==0:

k=k+1

if k == 0:

list.append(i)

else:

k = 0

legend =n/math.log(n)

print("Prime numbers count: ", len(list))

print("n/ln(n): ", legend)

print("Accuracy: ",legend/len(list))

return list

**Вывод**: в данной работе были рассмотрены основы теории чисел и их использование в криптографии, были исследованы и реализованы алгоритмы поиска простых чисел, нахождения НОД двух и трех чисел, каноническое разложение числа на простые множители. Также были рассмотрены алгоритмы модулярной арифметики, опробованы алгоритм Евклида, соотношение Безу и малая Теорема ферма.