**Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации**

**ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникации им. проф. М.А. Бонч-Бруевича»**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Факультет: ИКСС

Отчет по лабораторной работе №3

ТЕСТИРОВАНИЕ ПРОСТЫХ ЧИСЕЛ И НАХОЖДЕНИЕ КВАДРАТИЧНЫХ ВЫЧЕТОВ

Выполнил: Громов А.А.

Группа: ИКТЗ-83

Проверил: Яковлев В.А.

Санкт-Петербург

2021 г.

**Цель работы:**

Закрепить знания, полученные на лекциях курса “Основы криптографии с открытым ключом“ по разделам: “Квадратичные вычеты” и “Генерирование и тестирование простых чисел”.

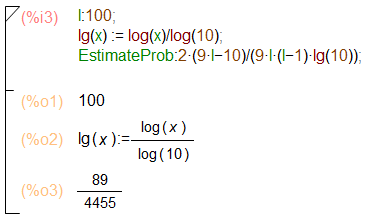
**Используемое ПО:**

wxMaxima

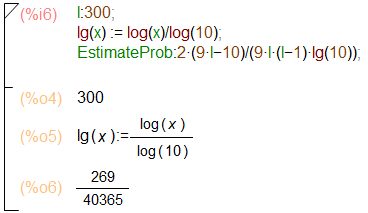
**Выполнение работы:**

**Задание 1**

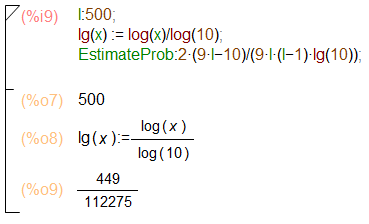
1. Перейти к пакету “Maxima”.
2. Рассчитать вероятность попадания на простое число при случайном генерировании чисел разрядности *l*=100, 300, 500 и 1000 при помощи следующей команды:



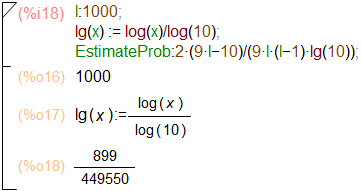
89/4455 ≈ 2%



269/40365 ≈ 0,7%



449/112275 ≈ 0,4%



899/449550 ≈ 0,2%

1. Для проверки теста Ферма сгенерировать необходимое количество случайных 3-х разрядных чисел:

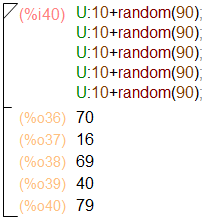




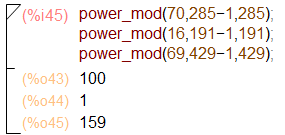


m = 285, 191(простое), 429

Сгенерировать не менее 5 случайных 2-х разрядных чисел *a*:

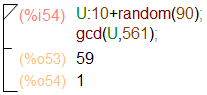
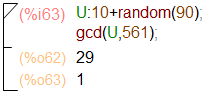
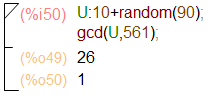
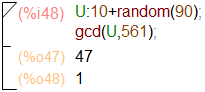


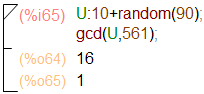
Произвести проверку чисел *m* на простоту, используя тест Ферма:



Проверка на простоту была проведена в основном верно, хотя встречаются ошибки.

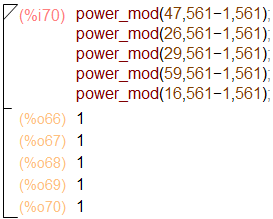
1. Произвести тестирования числа Кармайкла *m=561* по методу Ферма. Для этого сгенерировать необходимое количество случайных 2-х разрядных чисел по п. 3 и далее выбрать из них не менее 5 чисел *a’* взаимно простых с *561*





Сгенерированы числа 47, 26, 29, 59, 16.

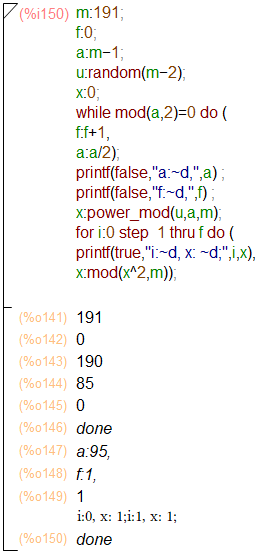
Проверить число *561,* используя тест Ферма:



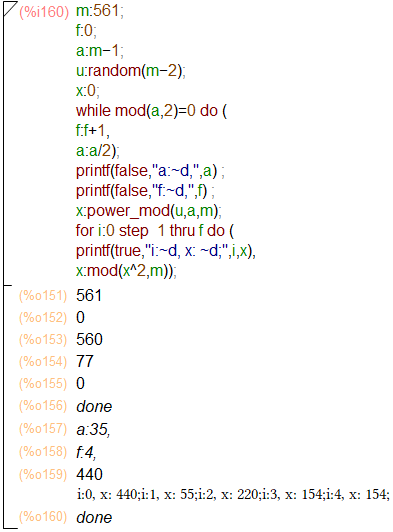
Проверка на простоту была выполнена абсолютно верно!

1. Произвести тестирование на простоту одного из чисел *m,* сгенерированных в п.3 и число Кармайкла 561, по методу Миллера–Рабина.

Выберем m = 191

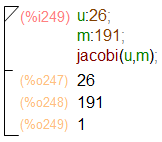
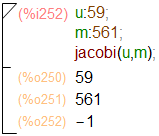


Выберем m = 561



Эффективность данного теста относительно теста Ферма оказалась выше, поскольку является его усовершенствованной версией и определяет числа Кармайкла.

1. Найти несколько квадратичных вычетов *u<m* по *mod(m),*где *m* одно из простых 3-х разрядных чисел, полученных в п. 5, используя вычисление символа Якоби ( который для простых *m* совпадает с символом Лежандра)

**Задание 2**

1. Распределите числа в поле GF(p) на вычеты и невычеты.

GF(13)

12 mod13 = 1

22 mod13 = 4

32 mod13 = 9

42 mod13 = 3

52 mod13 = 12

62 mod13 = 10

72 mod13 = 10

82 mod13 = 12

92 mod13 = 3

102 mod13 = 9

112 mod13 = 4

122 mod13 = 1

Вычеты: 1, 3, 4, 9, 10, 12

Невычеты: 2, 5, 6, 7, 8, 11

1. Проверьте, является ли число а=(№вар+20)mod31 вычетом по модулю 17, 19.

a = (4+20) mod 31 = 24 mod 31 = 24

Число 24 не принадлежит полям GF(17) и GF(19), по этой причине не может являться вычетом или невычетом. Поэтому вычисляем

24mod17 = 7

24mod19 = 5

По модулю 17: – невычет

По модулю 19: – вычет

1. Решите уравнение 
   1. Р = 23, а = 6

p = 4\*5+3

x = = 12

Ответ: (12, -12)

* 1. р = 29, а = 7

p = 4\*7+1

Подберем b такое, что b2 -1 – невычет. Пусть b=4 => b2-1 =15 - невычет

14 = 8 + 4 + 2

151 mod 29 = 15

152 mod 29 = 22

154 mod 29 = 20

158 mod 29 = 23

1514 mod 29 = 23\*20\*22 mod 29 = 28

x =

x =

15 = 8 + 4 + 2 + 1

71 mod 29 = 7

72 mod 29 = 20

74 mod 29 = 23

78 mod 29 = 7

715 mod 29 = 7\*23\*20\*7 mod 29 = 7

Ответ: (7, -7)

1. Решите уравнение 

n = 3\*7, a = 16

|  |  |
| --- | --- |
| *p = 4\*0+3*  *x* = 1, *x* = -1 | *p = 4\*1+3*  *x* = 4, *x* = -4 |

M = m1\*m2, M1 = M/m1, M2 = M/m2

N1 = M1-1 mod m1, N2 = M2-1 mod m2

X = (a1\*M1\*N1+ a2\*M2\*N2)modM

Системы уравнений:

*M = 3\*7 = 21*

*M1 = 21/3 = 7*

*M2 = 21/7 = 3*

*N1 = 7-1mod3 = 1*

*N2 = 3-1mod7 = 5*

X =

*M = 3\*7 = 21*

*M1 = 21/3 = 7*

*M2 = 21/7 = 3*

*N1 = 7-1mod3 = 1*

*N2 = 3-1mod7 = 5*

X = (-1\*7\*1+1\*3\*5) mod 21 = 8 mod 21 = 8

*M = 3\*7 = 21*

*M1 = 21/3 = 7*

*M2 = 21/7 = 3*

*N1 = 7-1mod3 = 1*

*N2 = 3-1mod7 = 5*

*X = (1\*7\*1-1\*3\*5) mod 21 = -8 mod 21 = 13*

*M = 3\*7 = 21*

*M1 = 21/3 = 7*

*M2 = 21/7 = 3*

*N1 = 7-1mod3 = 1*

*N2 = 3-1mod7 = 5*

*X = (-1\*7\*1-1\*3\*5) mod 21 = -22 mod 21 = 20*

Ответ: x = 1, x = 8, x = 13, x = 20

Проверка:

**Вывод:**

В данной лабораторной работы, мы закрепили полученные навыки по нахождению доли простых чисел заданной разрядности и генерированию простых чисел при вероятностном тестировании.

Еще были выполнены упражнения по нахождению квадратичных вычетов по простому модулю и по вычислению их квадратных корней, а также решены дополнительные задания.