МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего профессионального образования
«Южно-Уральский государственный университет (национальный исследовательский университет)»
Высшая школа электроники и компьютерных наук
Кафедра системного программирования

РАЗРАБОТКА ПРОГРАММНОЙ СИСТЕМЫ ДЛЯ ВЫЧИСЛЕНИЯ И АНАЛИЗА ДИСКРЕТНЫХ ЛОГАРИФМОВ ДЛЯ НАЧАЛЬНЫХ ДИАПАЗОНОВ ПРОСТЫХ ЧИСЕЛ

Автор:
студент группы КЭ-433
П.А. Бородин

Научный руководитель:
Профессор кафедры СП, д.ф.-м.н.,
доцент
Р.Ж. Алеев

АКТУАЛЬНОСТЬ

- Дискретные логарифмы применяются в криптографии в схемах асимметричного шифрования и криптографических протоколах.
- Необходимость решения задач, требующих большого количества вычислений.
- Результаты данного исследования способствуют расширению применения Python и Tkinter в области математики и научных вычислений.

ЦЕЛЬ И ЗАДАЧИ РАБОТЫ

Цель:

Разработка программной системы для вычисления и анализа дискретных логарифмов для начальных диапазонов простых чисел.

Задачи:

1. Составление списка простых чисел из диапазона [2..P] для заданного P.
2. Разработка функции для нахождения наименьшего примитивного корня R по модулю простых чисел из диапазона [2..P].
3. Разработка функции для нахождения и анализа всех дискретных R-логарифмов по модулю простых чисел из диапазона [2..P].
4. Разработка графического приложения, выполняющего все указанные функции.

НАИМЕНЬШИЙ ПРИМИТИВНЫЙ КОРЕНЬ

Примитивный корень по модулю p – это число, у которого при возведении его в степени от 1 до p в остатке получаются числа от 1 до p-1. Соответственно, наименьший примитивный корень – первый из примитивных корней.

Например:

$$
\begin{aligned}
3^1 &= 3 = 3^0 \times 3 \equiv 1 \times 3 = 3 \equiv 3 \pmod 7 \\
3^2 &= 9 = 3^1 \times 3 \equiv 3 \times 3 = 9 \equiv 2 \pmod 7 \\
3^3 &= 27 = 3^2 \times 3 \equiv 2 \times 3 = 6 \equiv 6 \pmod 7 \\
3^4 &= 81 = 3^3 \times 3 \equiv 6 \times 3 = 18 \equiv 4 \pmod 7 \\
3^5 &= 243 = 3^4 \times 3 \equiv 4 \times 3 = 12 \equiv 5 \pmod 7 \\
3^6 &= 729 = 3^5 \times 3 \equiv 5 \times 3 = 15 \equiv 1 \pmod 7 \\
3^7 &= 2187 = 3^6 \times 3 \equiv 1 \times 3 = 3 \equiv 3 \pmod 7
\end{aligned}
$$

Здесь мы видим, что остатки в периоде, равные 3, 2, 6, 4, 5, 1, образуют перестановку всех ненулевых остатков по модулю 7, подразумевая, что 3 действительно является примитивным корнем по модулю 7.

ДИСКРЕТНЫЕ R-ЛОГАРИФМЫ

Дискретный R-логарифм числа y – это такое число x, которое является решением сравнения $R^x \equiv y \pmod p$.

Например: найдем дискретные логарифмы для $3^x \equiv y \pmod{17}$

$3^1 \equiv 3$	$3^5 \equiv 5$	$3^9 \equiv 14$	$3^{13} \equiv 12$
$3^2 \equiv 9$	$3^6 \equiv 15$	$3^{10} \equiv 8$	$3^{14} \equiv 2$
$3^3 \equiv 10$	$3^7 \equiv 11$	$3^{11} \equiv 7$	$3^{15} \equiv 6$
$3^4 \equiv 13$	$3^8 \equiv 16$	$3^{12} \equiv 4$	$3^{16} \equiv 1$

Зная примитивный корень можно получить все дискретные логарифмы. Для этого возведем примитивный корень в степени от 1 до p-1. Также можно убедиться, что примитивный корень был определен верно (в остатке получаются числа от 1 до p-1).

ДИАГРАММА ВАРИАНТОВ ИСПОЛЬЗОВАНИЯ

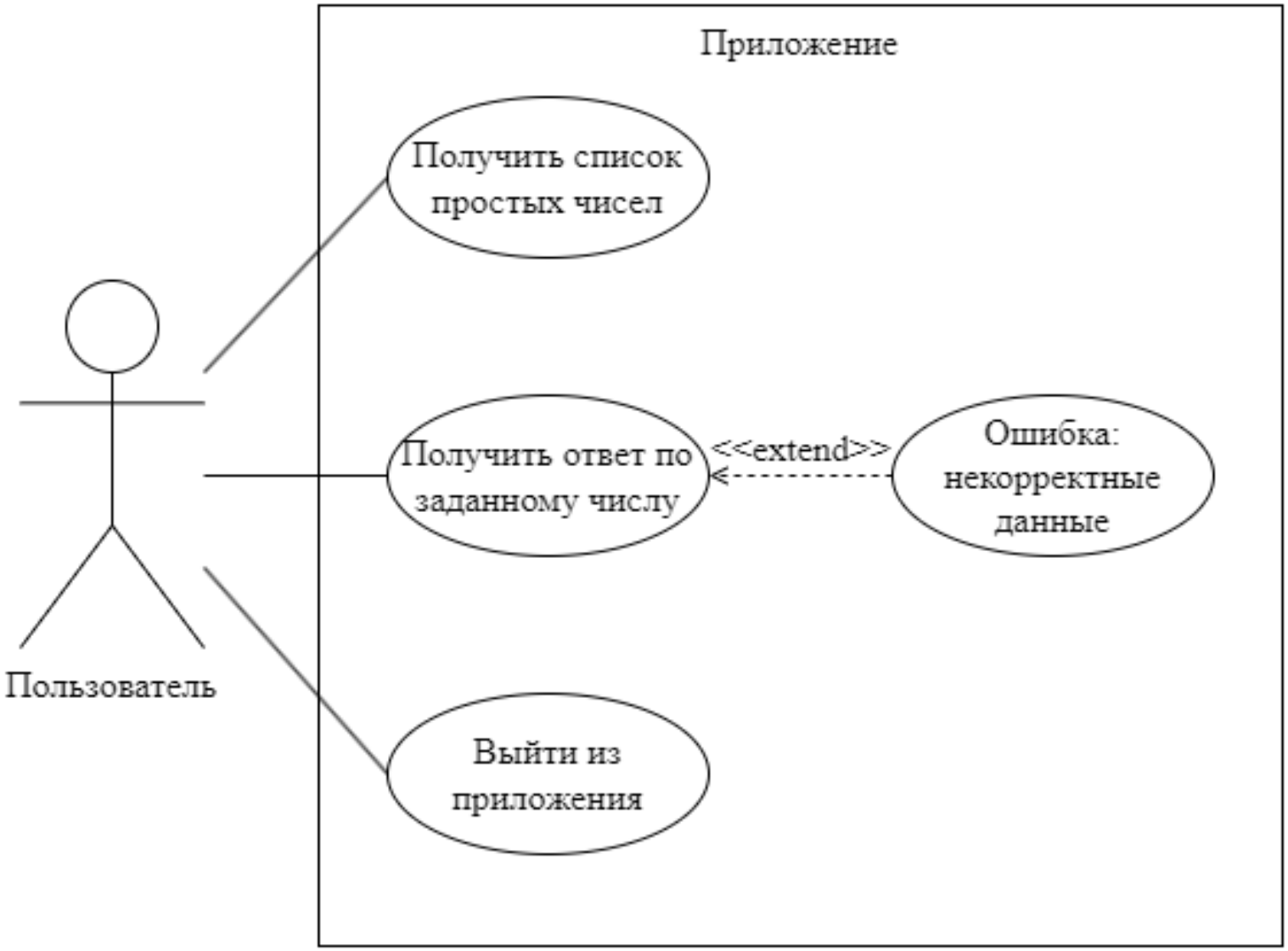
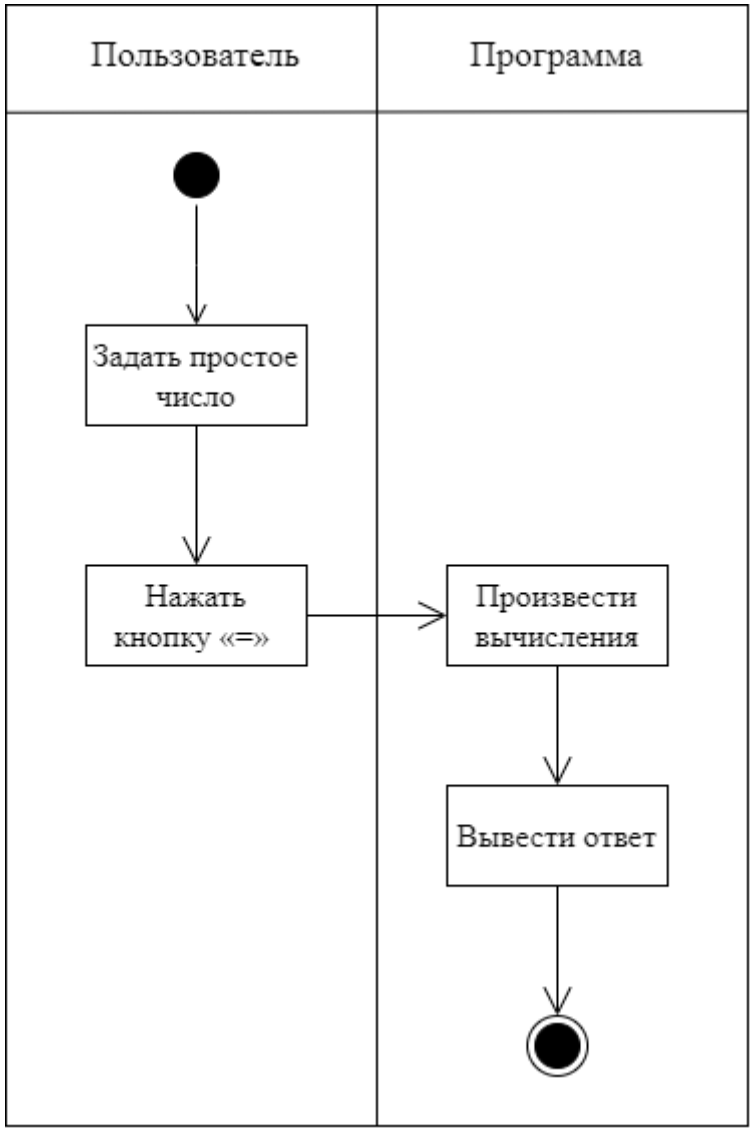


ДИАГРАММА ДЕЯТЕЛЬНОСТИ



СРЕДСТВА РАЗРАБОТКИ

Язык программирования:

Python 3.12.2

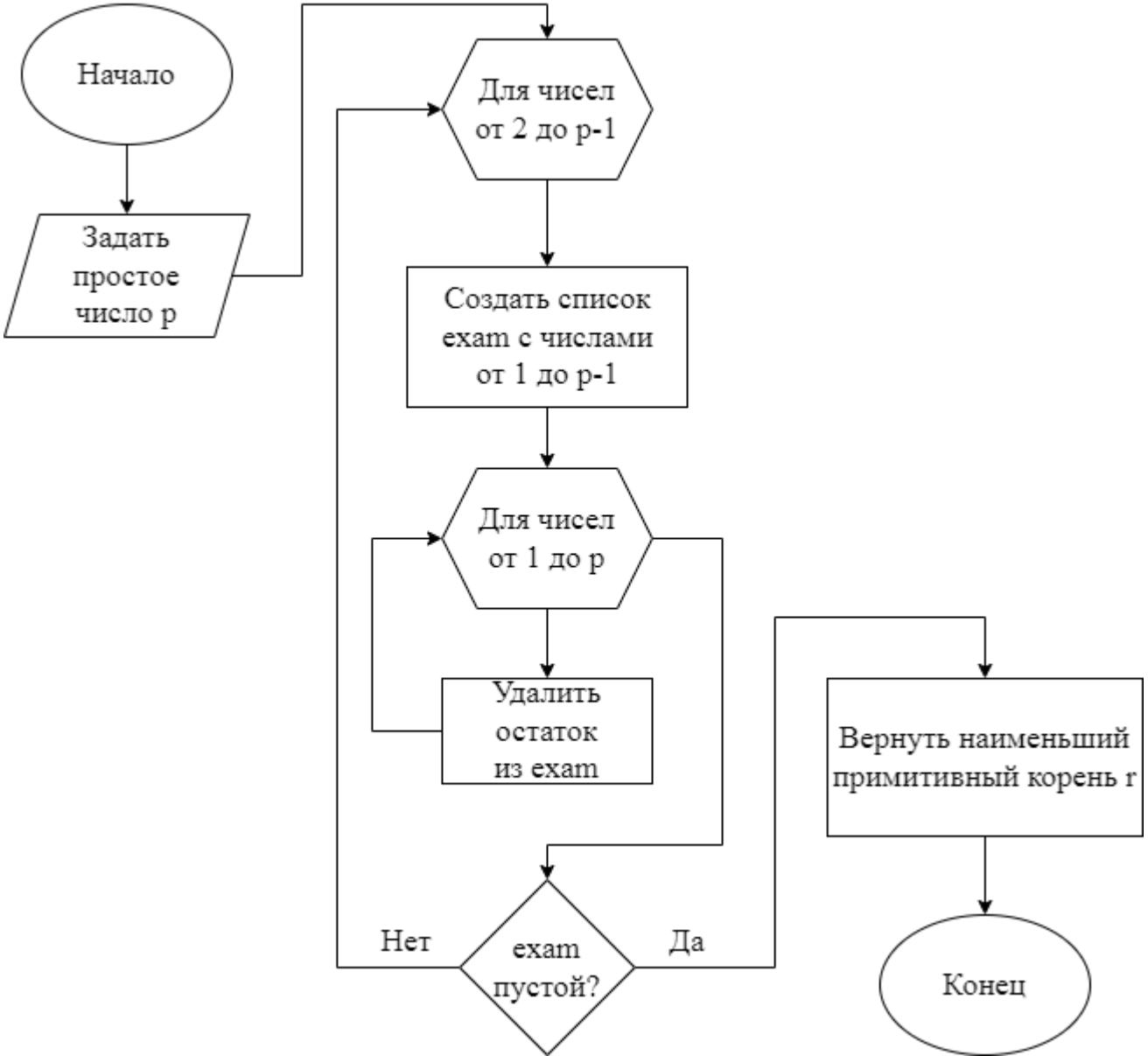
Среда разработки:

PyCharm Community Edition 2023.2.6

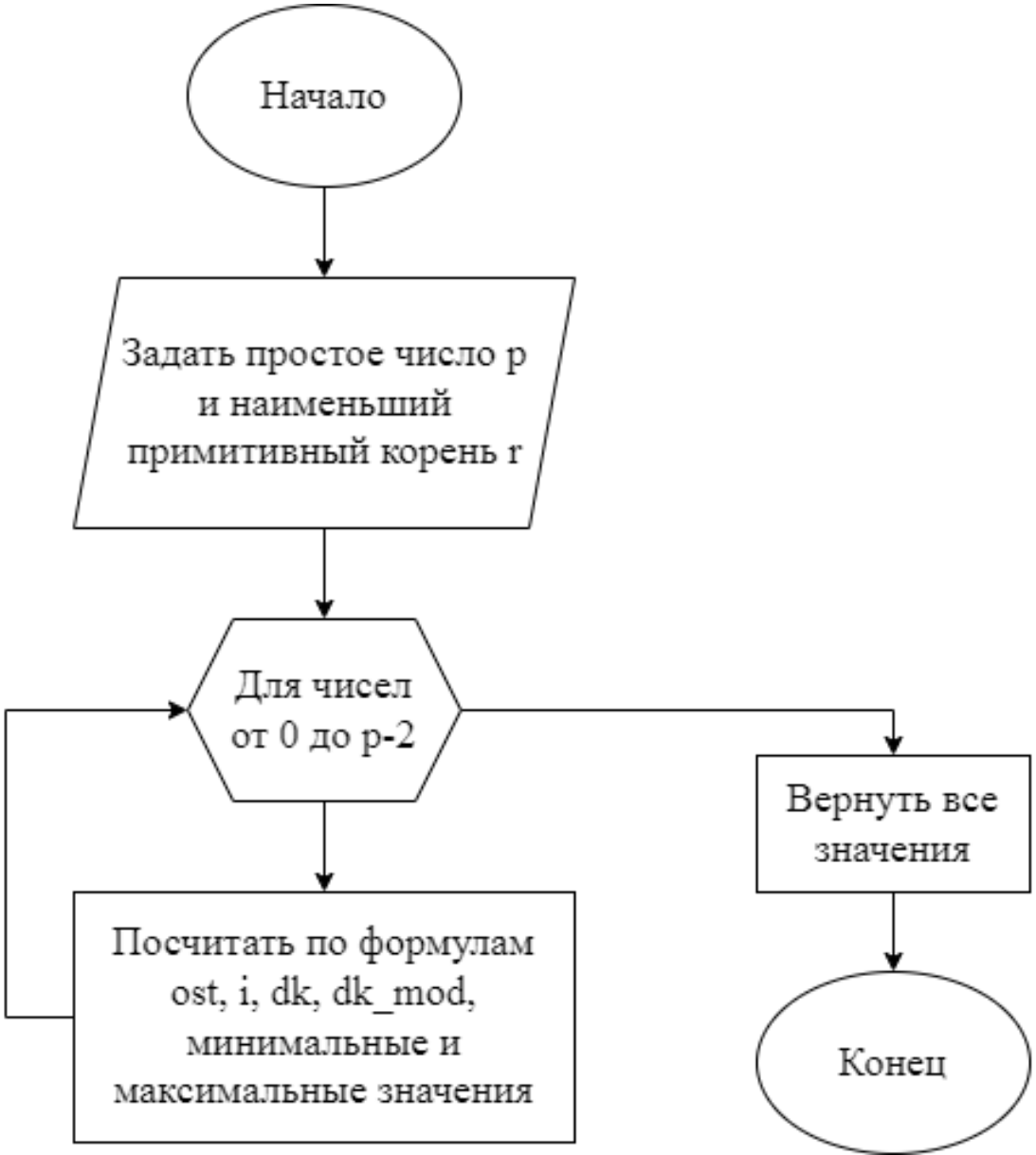
Используемые библиотеки:

Tkinter 8.6.13

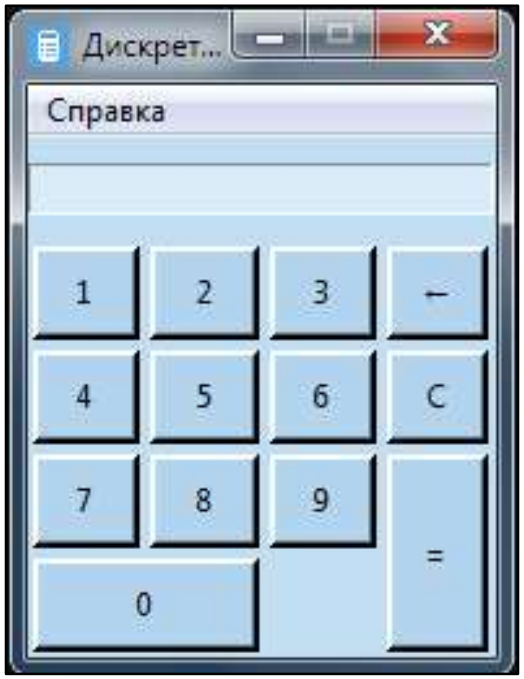
АЛГОРИТМ НАХОЖДЕНИЯ НАИМЕНЬШЕГО ПРИМИТИВНОГО КОРНЯ

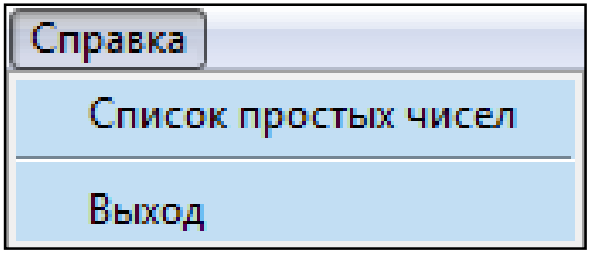


АЛГОРИТМ НАХОЖДЕНИЯ ДИСКРЕТНЫХ ЛОГАРИФМОВ

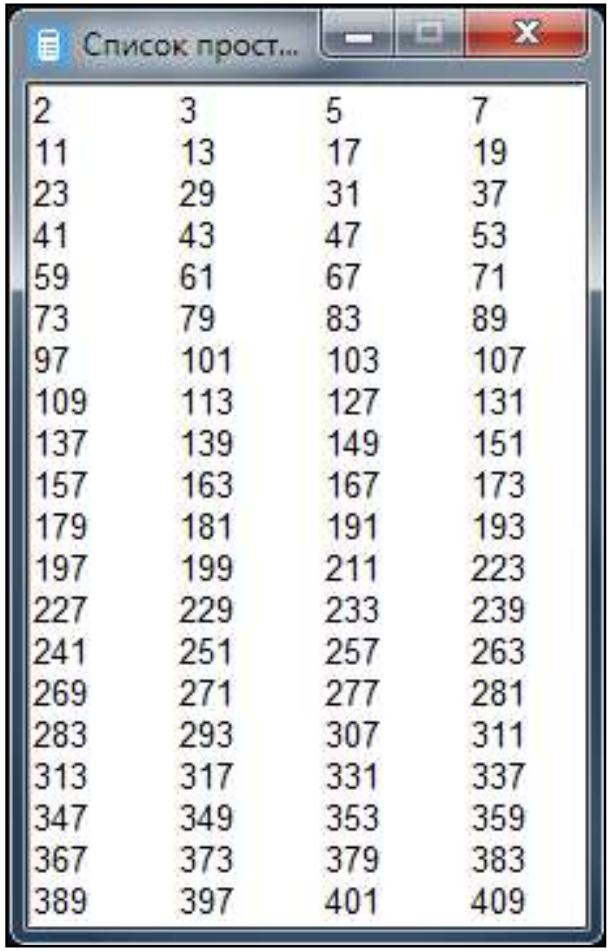


МОДЕЛЬ ГЛАВНОГО ОКНА ПРИЛОЖЕНИЯ

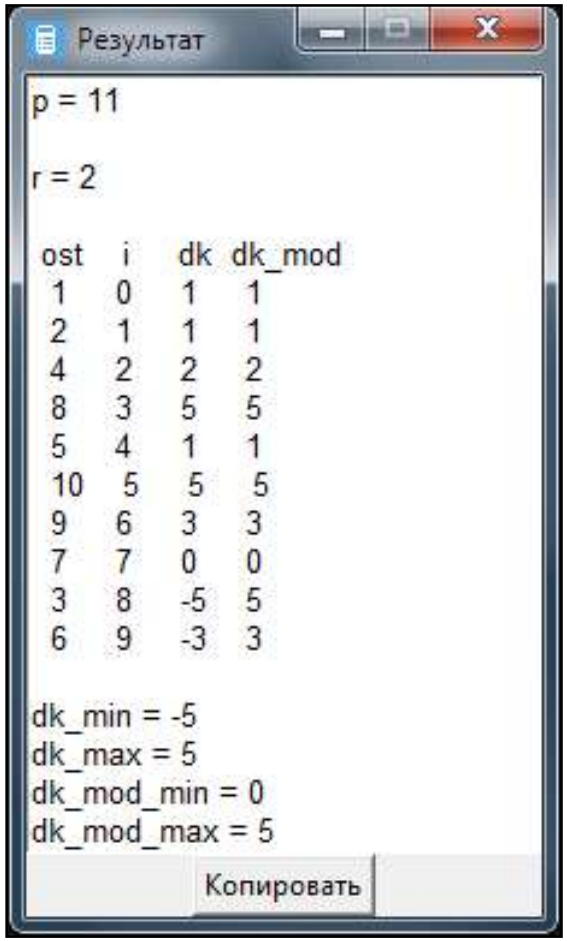


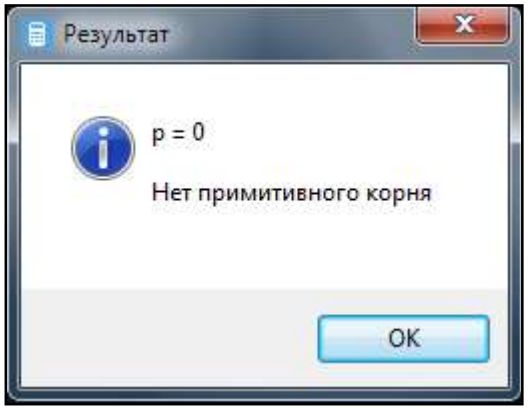


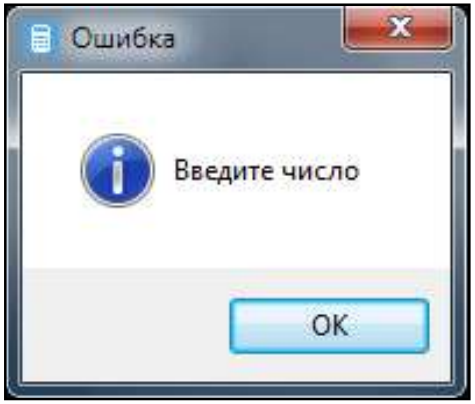
МОДЕЛЬ ОКНА СО СПИСКОМ ПРОСТЫХ ЧИСЕЛ



МОДЕЛИ ОКОН С ВЫВОДОМ РЕЗУЛЬТАТА







d(k) – разность остатка k и степени числа, $k \equiv R^x \pmod{p}$.

ТЕСТИРОВАНИЕ СИСТЕМЫ

Тесты на корректность входных и выходных данных.

№	Работа программы	Ожидаемый результат	Тест
1	Ввод: 7 Вывод: r = 3, dk_min = 0, dk_max = 3, dk_mod_min = 0, dk_mod_max = 3	Ввод: 7 Вывод: r = 3, dk_min = 0, dk_max = 3, dk_mod_min = 0, dk_mod_max = 3	Пройден
2	Ввод: 23 Вывод: r = 5, dk_min = -13, dk_max = 15, dk_mod_min = 0, dk_mod_max = 15	Ввод: 23 Вывод:r = 5, dk_min = -13, dk_max = 15, dk_mod_min = 0, dk_mod_max = 15	Пройден
3	Ввод: 50 Вывод: Нет примитивного корня	Ввод: 50 Вывод: Нет примитивного корня	Пройден
4	Ввод: -23 Вывод: Нет примитивного корня	Ввод: -23 Вывод: Нет примитивного корня	Пройден
5	Ввод: +23 Вывод: r = 5, dk_min = -13, dk_max = 15, dk_mod_min = 0, dk_mod_max = 15	Ввод: +23 Вывод: r = 5, dk_min = -13, dk_max = 15, dk_mod_min = 0, dk_mod_max = 15	Пройден
6	Ввод: тест Вывод: Введите число	Ввод: тест Вывод: Введите число	Пройден

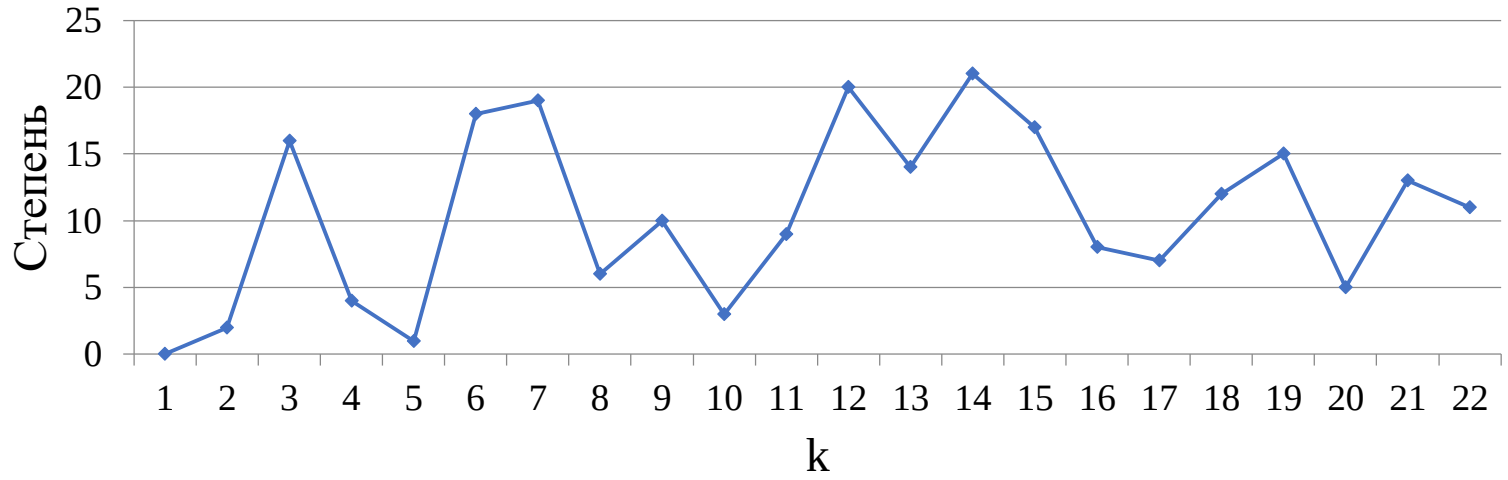
РЕЗУЛЬТАТЫ

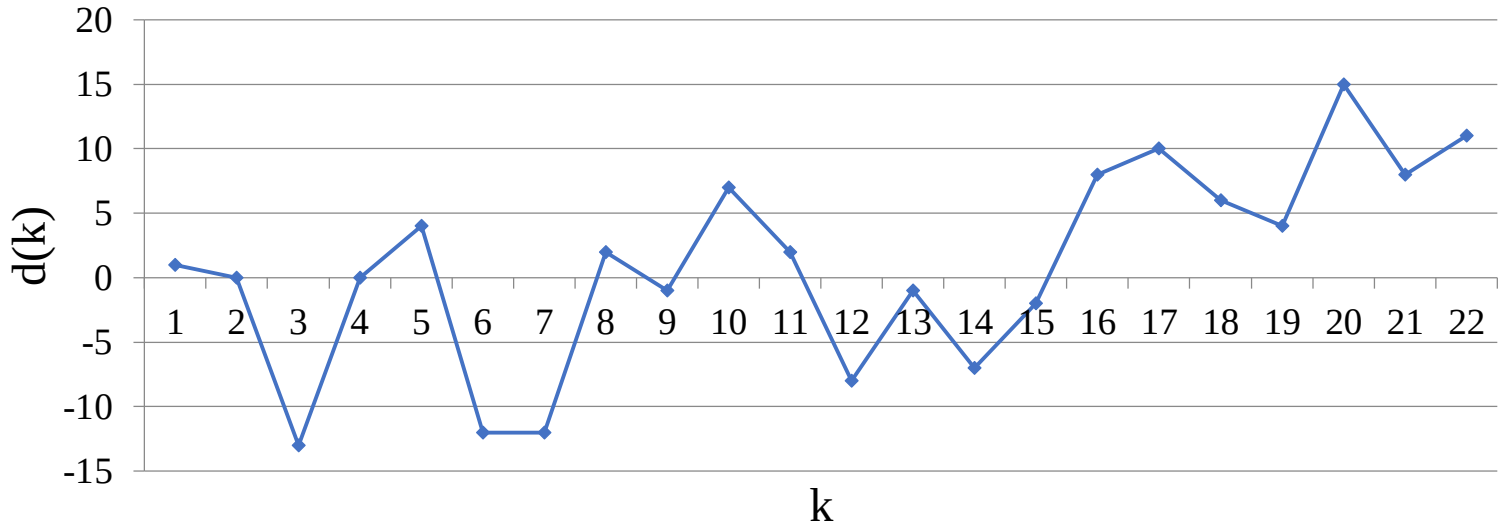
Результаты в виде таблицы для p = 23.

По возрастанию k				По возрастанию степени			
k	**Степень**	**d(k)**	**|d(k)|**	**Степень**	**k**	**d(k)**	**|d(k)|**
1	0	1	1	0	1	1	1
2	2	0	0	1	5	4	4
3	16	-13	13	2	2	0	0
4	4	0	0	3	10	7	7
5	1	4	4	4	4	0	0
6	18	-12	12	5	20	15	15
7	19	-12	12	6	8	2	2
8	6	2	2	7	17	10	10
9	10	-1	1	8	16	8	8
10	3	7	7	9	11	2	2
11	9	2	2	10	9	-1	1
12	20	-8	8	11	22	11	11
13	14	-1	1	12	18	6	6
14	21	-7	7	13	21	8	8
15	17	-2	2	14	13	-1	1
16	8	8	8	15	19	4	4
17	7	10	10	16	3	-13	13
18	12	6	6	17	15	-2	2
19	15	4	4	18	6	-12	12
20	5	15	15	19	7	-12	12
21	13	8	8	20	12	-8	8
22	11	11	11	21	14	-7	7
Минимум		-13	0	**Минимум**		-13	0
Максимум		15	15	**Максимум**		15	15

РЕЗУЛЬТАТЫ

Результаты в виде графиков для p = 23.





АНАЛИЗ ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ

1. Были проведены вычисления для диапазонов с большими значениями.
2. Найдены все дискретные R-логарифмы по модулю простых чисел до 1000.
3. На основе полученных данных составлены таблицы и построены графики.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ

1. Составлен список простых чисел из диапазона [2..1000].
2. Разработана функция для нахождения наименьшего примитивного корня R по модулю простых чисел из диапазона [2..1000].
3. Разработана функция для нахождения и анализа всех дискретных R-логарифмов по модулю простых чисел из диапазона [2..1000].
4. Разработано графическое приложение со всеми указанными функциями.

РЕЗУЛЬТАТЫ

Результаты в виде графиков для p = 23.