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

РАЗРАБОТКА ПРОГРАММНОЙ СИСТЕМЫ ДЛЯ ИЗУЧЕНИЯ КРУГОВЫХ ЕДИНИЦ ДЛЯ ПРОСТЫХ ЧИСЕЛ

Рецензент

Доцент кафедры компьютерной топологии и алгебры ФГБОУ ВО «ЧелГУ», к.ф.-м.н.

О.В. Митина

Научный руководитель,

профессор кафедры СП, д.ф.-м.н., доцент

Р.Ж. Алеев

Автор:

Студент группы КЭ-220

Я.П. Романов

Челябинск 2024

АКТУАЛЬНОСТЬ

- **Теория чисел:** работа с тригонометрическими функциями и решение сложных задач, связанных с волнами, колебаниями, электричеством, магнетизмом, оптикой и др.
- **Криптография:** алгоритмы для шифрования, создание криптографических ключей, электронных цифровых подписей
- **Машинное обучение:** используются в задачах классификации или регрессии для представления угла или направления

ЦЕЛЬ И ЗАДАЧИ ИССЛЕДОВАНИЯ

Цель

Разработка программной системы для изучения круговых единиц для простых чисел.

Задачи

- Изучение предметной области
- Проведение вычислений
- Определение функциональных и нефункциональных требований к системе
- Разработка и реализация алгоритмов расчетов
- Определение способа вывода данных
- Тестирование системы

АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

- Определение. Целые числа k и l сравнимы по натуральному модулю m, если $k - l$ делится на m.
- Пусть n и m – натуральные числа. Число n называется примитивным первообразным корнем по модулю m, если для любого натурального числа k, взаимно простого с m, существует такое натуральное число j_k, что $n^{j_k} \equiv k \ (mod\ m)$
- Пусть p – простое число, g – примитивный корень по модулю p и α – примитивный корень из единицы степени p. Круговой единицей для примитивного корня g называется комплексное число

$$1 + \alpha + \cdots + \alpha^{g-1}.$$

- Пусть p – простое число и α – примитивный корень из единицы степени p. Также пусть $\lambda = l_0 * 1 + l_1\alpha + l_2\alpha^2 + \cdots + l_{p-1}\alpha^{p-1}$, где для любого j∈{0,1,…,p-1} коэффициент l_j – рациональное число. Следом комплексного числа λ называется рациональное число

$$l_0(p-1) - l_1 - l_2 - \cdots - l_{p-1}.$$

ФОРМИРОВАНИЕ ИСХОДНЫХ ДАННЫХ ДЛЯ СИСТЕМЫ

1. Задается простое число
2. Рассчитываются следы степеней круговых единиц сравнимые с 1 по модулю p
3. Рассчитываются следы степеней круговых единиц по модулям 2 и 3
4. Находим степени, удовлетворяющие пунктам 2 и 3

ФОРМИРОВАНИЕ ИСХОДНЫХ ДАННЫХ ДЛЯ СИСТЕМЫ

Задается простое число p

```
gap> p:=11;
11
```

Вычисляется наименьший примитивный корень g по модулю p

```
gap> g:=PrimitiveRootMod(p);
2
```

Круговая единица

```
gap> c:=1+E(p);
-E(11)^2-E(11)^3-E(11)^4-E(11)^5-E(11)^6-E(11)^7-
E(11)^8-E(11)^9-E(11)^10
```

ФОРМИРОВАНИЕ ИСХОДНЫХ ДАННЫХ ДЛЯ СИСТЕМЫ

Проверим, что след числа $c^{(p-1)/2}$ сравним с $p-1$ по модулю p

```
gap> Trace(c^((p-1)/2)) mod p;
1
```

Находим порядки 2 и 3 по модулю p

```
gap> f2:=OrderMod(2,p);
10
gap> f3:=OrderMod(3,p);
5
```

Эти числа обеспечивают делимость на 2 и 3 коэффициентов чисел $\pm c^k - 1$.

ФОРМИРОВАНИЕ ИСХОДНЫХ ДАННЫХ ДЛЯ СИСТЕМЫ

Сначала для 2

```
gap> st:=2^f2-1;
1023
gap> lu2:=CoeffsCyc(c^st-1,p) mod 2;
[ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 ]
```

Пытаемся уменьшить число st

```
gap> FactorsInt(st);
[ 3, 11, 31 ]
gap> st3:=st/3;
341
gap> st11:=st/11;
93
gap> st31:=st/31;
33
```

ФОРМИРОВАНИЕ ИСХОДНЫХ ДАННЫХ ДЛЯ СИСТЕМЫ

gap> lu2:=CoeffsCyc(c^st3-1,p) mod 2;
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
gap> lu2:=CoeffsCyc(c^st11-1,p) mod 2;
[0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1]
gap> lu2:=CoeffsCyc(c^st31-1,p) mod 2;
[0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0]
Подходит только $st3$
Находим наименьшее общее кратное чисел $(p-1)/2$ и $st3$
gap> ep2:=LcmInt((p-1)/2,st3);
1705

ФОРМИРОВАНИЕ ИСХОДНЫХ ДАННЫХ ДЛЯ СИСТЕМЫ

Проводим проверку

```
gap> tr:=Trace(c^ep2) mod p;
1
gap> tr:=Trace(-c^ep2) mod p;
10
gap> l2:=CoeffsCyc(c^ep2-1,p) mod 2;
[ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 ]
gap> l2:=CoeffsCyc(-c^ep2-1,p) mod 2;
[ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 ]
```

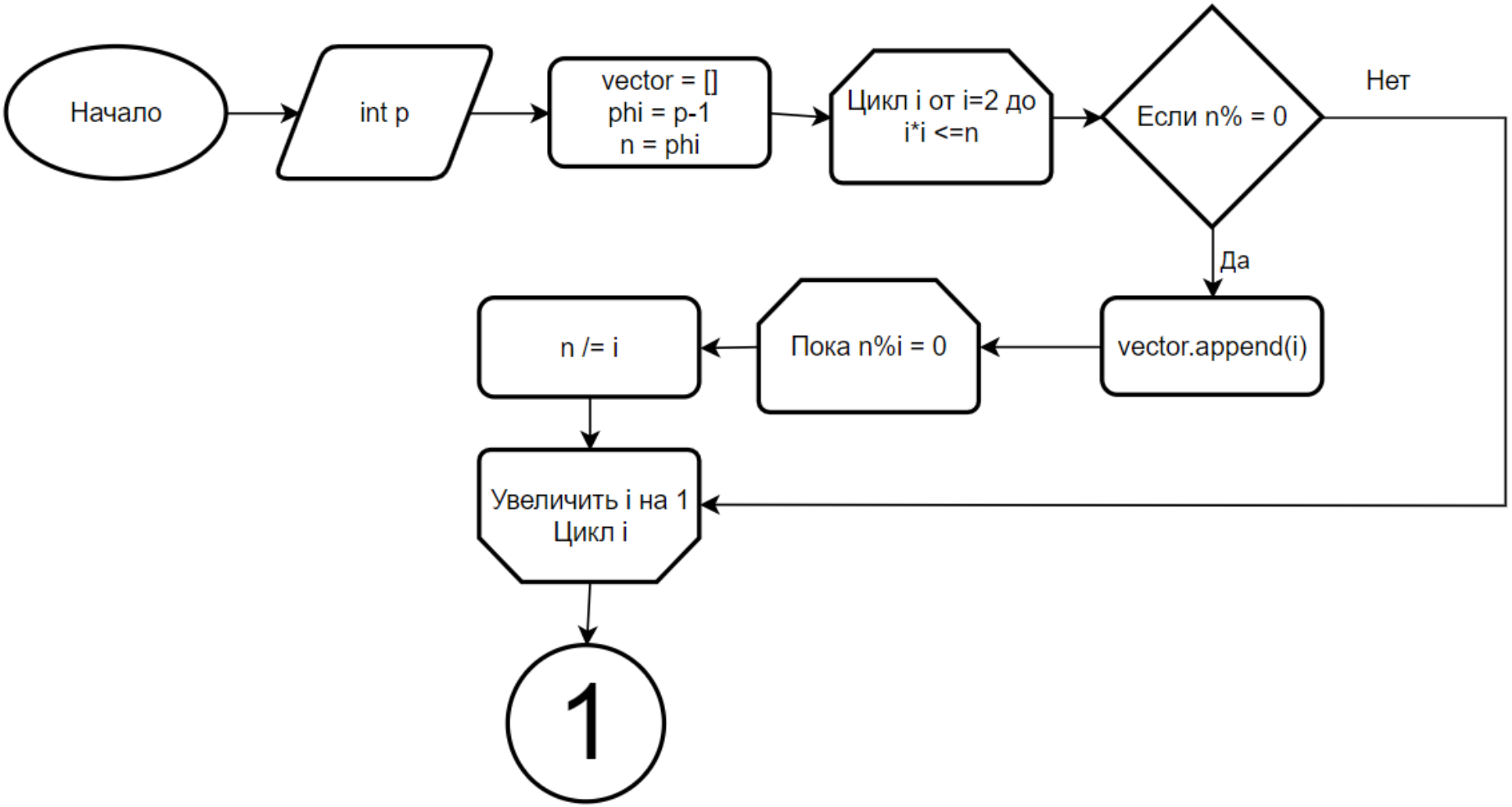
Проводим такие же вычисления для 3

СРЕДСТВА РАЗРАБОТКИ

- **Вычисления:** GAP 4.12.0
- **Язык программирования:** Python 3.9
- **Редактор кода:** PyCharm
- **Фреймворк:** Flask

ДИАГРАММА ВАРИАНТОВ ИСПОЛЬЗОВАНИЯ

АЛГОРИТМ ВЫЧИСЛЕНИЯ ПРИМИТИВНОГО КОРНЯ



АЛГОРИТМ ВЫЧИСЛЕНИЯ ПРИМИТИВНОГО КОРНЯ

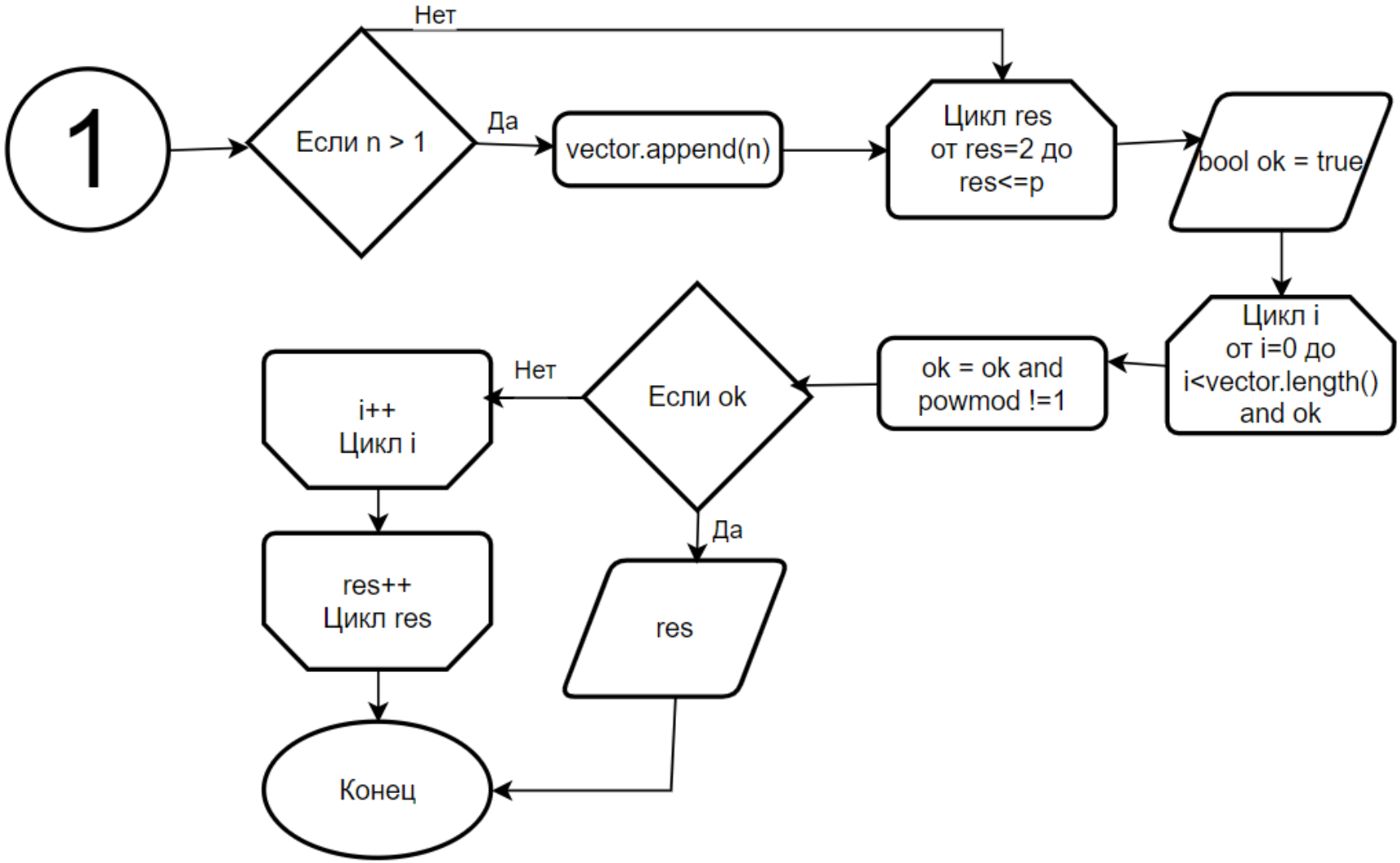


СХЕМА БАЗЫ ДАННЫХ

System	
PK	ID INT
	p INT
	g INT
	trace INT
	f2 INT
	f3 INT
	F2 VARCHAR(2000)
	F3 VARCHAR(2000)
	ep2 VARCHAR(2000)
	ep3 VARCHAR(2000)
	for2 VARCHAR(2000)
	for3 VARCHAR(2000)

ДЕМОНСТРАЦИЯ СИСТЕМЫ

System

	p	g	trace	f2	f3	F2	F3	ep2	ep3	for2	for3
2	11	2	1	10	5	341	121	1705	605	-c^ep2	-c^ep3

Submit

ТЕСТИРОВАНИЕ

Функциональное тестирование было проведено на персональном компьютере с ОС Windows 10.

Было проведено 6 функциональных тестов.

Тестирование системы прошло успешно и все тесты были пройдены.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ

- Изучена предметная область
- Проведены вычисления
- Определены функциональные и нефункциональные требования к системе
- Разработаны и реализованы алгоритмы расчетов;
- Определен способ вывода данных;
- Проведено тестирование системы.