МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение

высшего профессионального образования

**«Дальневосточный федеральный университет»**

**ШКОЛА ЕСТЕСТВЕННЫХ НАУК**

**Кафедра прикладной математики, механики, управления и программного обеспечения**

**О Т Ч Е Т**

по индивидуальному заданию по дисциплине “Алгебра”

|  |
| --- |
| Выполнил студент гр. Б8204  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Д. А. Федоренко |
| Проверил к.т.н. доцент  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.Г. Чеканов |

г. Владивосток

2018

**Неформальная постановка задачи**

Построить простое расширение поля степени 3 с помощью неприводимого многочлена степени 3 над полем , а именно:

1. Написать программу для вычислений в поле для представления элементов расширения в виде многочленов от корня.
2. Проверить, является ли корень соответствующего многочлена примитивным элементом поля .
3. Написать программу для вычислений в расширении при матричном представлении элементов поля .

Многочлен: 1101

**Спецификация структур**

struct **field** {

int deg;

};

- Поле остатков по модулю простого числа

- Хранит значение порядка поля

struct **polynom** {

int deg;

matrix\* mat;

};

* Полином
* Хранит значение степени полинома и свою сопровождающую матрицу

**Спецификация функций**

vector<matrix> **exp** (field F, polynom P)

* Строит расширение поля сопровождающей матрицей полинома
* На вход принимает поле F и полином P
* Возвращает расширение поля в виде матрицы

Принцип работы:

Происходит формирование расширения поля по принципу:

E + A + , где E – единичная матрица порядка A, A – матрица для неприводимого многочлена.

bool **checkPrimitive** (vector<matrix> F, matrix m)

* Проверяет является ли элемент примитивным
* На вход принимает расширение поля F и элемент m, который надо проверить на примитивность
* Возвращает логическое значение: true или false

Принцип работы:

Проверяется есть ли в расширении поля F элементы, которые являются элементом m в степени простого числа, если есть такие элементы, то элемент m – примитивный, иначе нет.