1. 7Министерство науки и высшего образования Российской Федерации
2. Санкт-Петербургский политехнический университет Петра Великого
3. Институт компьютерных наук и кибербезопасности
4. Высшая школа кибербезопасности

**ЛАБОРАТОРНАЯ РАБОТА № 3**

1. «Разложение на множители многочленов от одной переменной над полем Галуа»
2. по дисциплине «Быстрые вычислительные алгоритмы»
3. Выполнил
4. студент гр. 5151001/00201 Устюгов А.А.

<*подпись*>

1. Преподаватель д.т.н. Шенец Н.Н.

<*подпись*>

1. Санкт-Петербург
2. 2024

# Цель работы

Изучение алгоритмов нахождения корней многочленов от одной переменной над полем Галуа и алгоритмов разложения на множители таких многочленов.

# Задание

1. Написать программу, реализующую вероятностный алгоритм поиска корней многочлена от одной переменной над простым полем Галуа.
2. Написать программу, реализующую алгоритм разложения на множители многочлена от одной переменной над полем Галуа.

# Ход работы

Обе программы были написаны с помощью SageMath.

В программе 1 необходимо реализовать вероятностный алгоритм поиска корней. В алгоритме мы находим нетривиальные делители с помощью взятия НОД от заданного многочлена и многочлена, задающего все поле. Затем, если НОД линейный, то корень найден, если НОД совпадает с заданным многочленом, то корни – все элементы поля, иначе итеративно начинаем раскладывать многочлен на нетривиальные делители с помощью того же НОД.

На рисунках 1,2,3 представлены некоторые тесты алгоритма

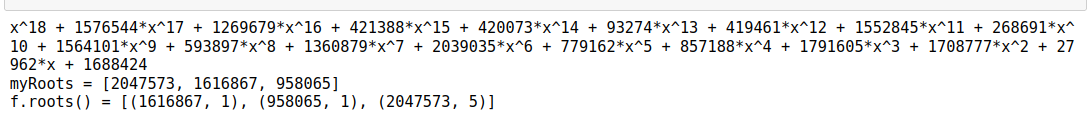


Рисунок 1 – тест из методического пособия

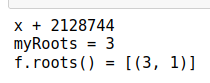


Рисунок 2 – поиск корня у линейного многочлена

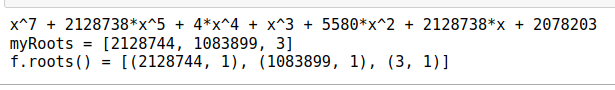


Рисунок 3 ­­– случайный многочлен

В программе 2 необходимо реализовать алгоритм Берлекэмпа разложение многочлена на множители. Основная идея алгоритма состоит в поиске f-разлагающего алгоритма. Его поиски основаны на линейной алгебре. Строится матрица, состоящая из коэффициентов многочленов *x\*\*(i\*q)*, затем ищутся собственные векторы с собственным числом 1. В результате мы и получим f-разлагающие многочлены. Далее, с его помощью и знанием того, что НОД от произведения это произведение НОДов, начинается поиск нетривиальных делителей заданного многочлена циклом по всем элементам поля.

На рисунках 4, 5, 6 представлены некоторые тесты.

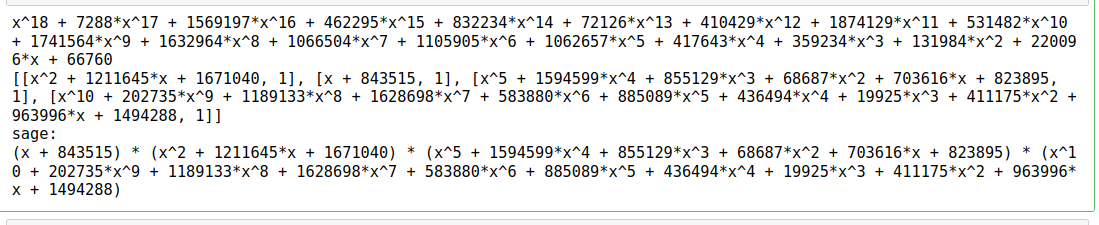


Рисунок 4 – тест из методического пособия

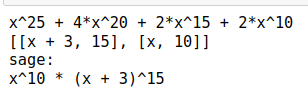


Рисунок 5 – тест с производной равной 0

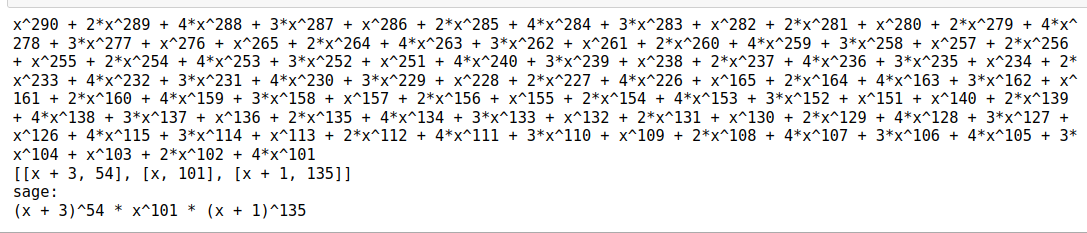


Рисунок 6 – смешанный тест

# Контрольные вопросы

1. Можно ли адаптировать вероятностный алгоритм нахождения корней многочлена от одной переменной над простым полем Галуа на случай полей ?
2. Для каких полей метод Берлекэмпа разложения многочленов на множители будет эффективен?

Для полей с небольшим числом элементов в поле, т.к. есть цикл по всем элементам поля.

1. Можно ли применить метод Кантора-Цассенхауза для конечных полей общего вида ?

# Вывод

В ходе выполнения лабораторной работы были изучены алгоритмы поиска корней и разложения многочлена на множители в конечном поле. Были реализованы вероятностный алгоритм нахождения корней многочлена от одной переменной и алгоритм Берлекэмпа разложения многочлена на множители.