### Министерство науки и высшего образования Российской Федерации

1. Санкт-Петербургский политехнический университет Петра Великого
2. —
3. Институт компьютерных наук и кибербезопасности
4. Высшая школа кибербезопасности

**ЛАБОРАТОРНАЯ РАБОТА № 2**

1. **«Расчет числа точек эллиптической кривой»**
2. по дисциплине «Методы алгебраической геометрии в криптографии»
3. Выполнил
4. студент гр. 5151001/00201 Устюгов А.А.

<*подпись*>

1. Проверил:
2. старший преподаватель Ярмак А.В.

<*подпись*>

1. Санкт-Петербург
2. 2023

# Цель работы

Изучение методов расчета числа точек эллиптических кривых, заданных над конечным полем.

# Порядок выполнения работы

1. Получить у преподавателя вариант задания и разработать программу П-1, реализующую алгоритм Чуфа расчета числа точек эллиптической кривой, заданной над конечным полем характеристики *p*.

2. Построить произвольное расширение поля и вычислить число точек эллиптической кривой над расширенным полем.

# Ход работы

В ходе данной лабораторной работы необходимо реализовать алгоритм Чуфа для подсчета числа точек эллиптической кривой.

Суть алгоритма Чуфа состоит в том, чтобы вычислить след эндоморфизма Фробениуса по модулю малых простых чисел, а затем с помощью к.т.о. собрать результирующий след и с его помощью посчитать количество точек. В ходе работы при вычислении эндоморфизма Фробениуса по модулю малых простых были использованы полиномы деления. Однако, из-за этого мне не удалось проверять характеристики поля больше чем 2\*\*20, так как не хватало памяти для их хранения.

Параметры эллиптической кривой:

p = 524347;

A = 15, B = 3;

Результаты вычислений эндоморфизма Фробениуса для всех li:

l[i] = 2

my trace = 0

l[i] = 3

my trace = -1

l[i] = 5

my trace = 3

l[i] = 7

0-point

my trace = 0

l[i] = 11

my trace = 7

l[i] = 13

my trace = 1

Результирующий T = -532;

Число точек N = 524880;

Характеристическое уравнение отображения Фробениуса:

Корнями являются [(-266.000000000000 - 673.491648055119\*I), (-266.000000000000 + 673.491648055119\*I)], где I-мнимая единица.

Посчитать число точек над расширением поля можно с помощью следующей формулы:

*, где – корни характеристического уравнения, m-степень расширения.* Было построено расширение 3 степени исходного поля. Количество точек над расширенным полем равно 1.44163846254441e17.

# Ответы на контрольные вопросы

1. Показать, что НОД(, где ­ – полином деления, построенный для кривой над . Какие координаты будут иметь точки порядка 3?

*,* далее необходимо убедится, что . Это действительно так: , следовательно, НОД(*.*

Точки порядка 3 будут иметь координаты (0 : 1 : 1) и (0 : 6 : 1)

2. Пусть . Найти

Характеристическое уравнение:

Его корни:

Тогда

3. По теореме Хассе число точек эллиптической кривой над близко к *p.* Показать, что для число точек на кривой равно *p+1.*

Число точек с учетом бесконечно удаленной можно найти по формуле

C учетом того ,что , посчитаем чему равно , следовательно, что , тогда в сумме все слагаемые уничтожатся и число точек равно p+1.

4. Показать, что если полином имеет корень в поле , то у кривой над полем четное число точек.

Число точек

Точка порядка 2 выглядит как (x, 0), а так как у полинома есть корень в то такая точка найдется, следовательно над полем четное число точек.

# Выводы

В данной лабораторной работе был изучен процесс подсчета числа точек эллиптической кривой с помощью алгоритма Чуфа, а также подсчета числа точек над расширением поля.