**Московский авиационный институт**

# (национальный исследовательский университет)

Институт №8 «Информационные технологии и прикладная математика»

Кафедра 806 «Вычислительная математика и программирование»

Дисциплина «Криптография»

# Лабораторная работа №3

Тема: Эллиптические кривые

|  |  |
| --- | --- |
| Студент: | Глушатов И.С. |
| Группа: | М8О-307Б-19 |
| Преподаватель: | Борисов А. В. |
| Дата: |  |
| Оценка: |  |

**Цель работы:** приобрести знания в области эллиптических кривых, написать программу, которая умеет складывать точки на эллиптических кривых с заданными коэффициентами над конечным полем и определять порядок точек.

**Задание:**

Подобрать такую эллиптическую кривую, порядок точки которой полным перебором находится за 10 минут на ПК. Упомянуть в отчёте результаты замеров работы программы, характеристики вычислителя. Также указать какие алгоритмы и/или теоремы существуют для облегчения и ускорения решения задачи полного перебора. Рассмотреть для случая конечного простого поля Z\_p

**Оборудование:** Домашний компьютер, процессор Intel® CoreTM i5-7200 CPU 3.40GHz 3.40 GHz, память 8ГБ, 64-разрядная система

**Ход работы**

Каноническая форма эллиптической кривой над конечным полем :

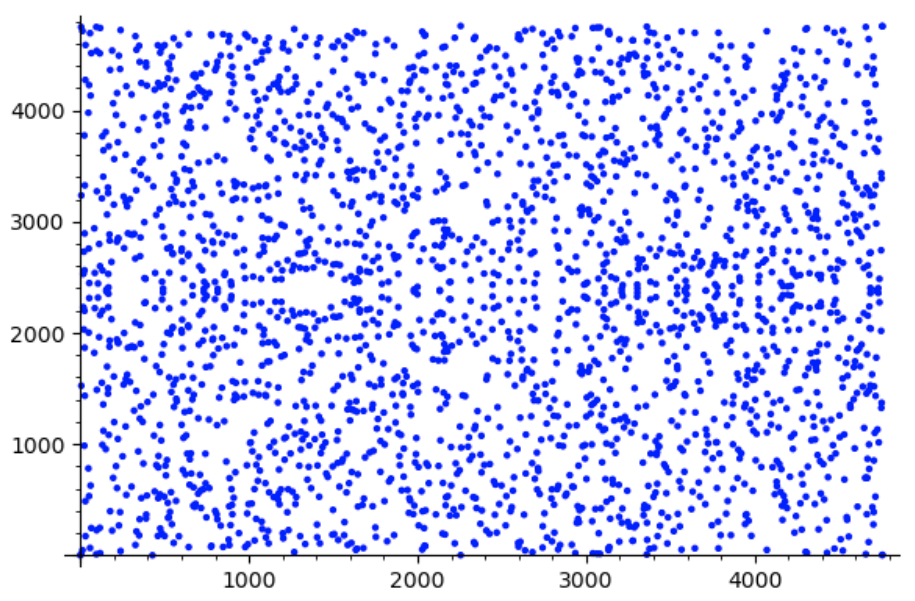
Сложение точек:

Пусть

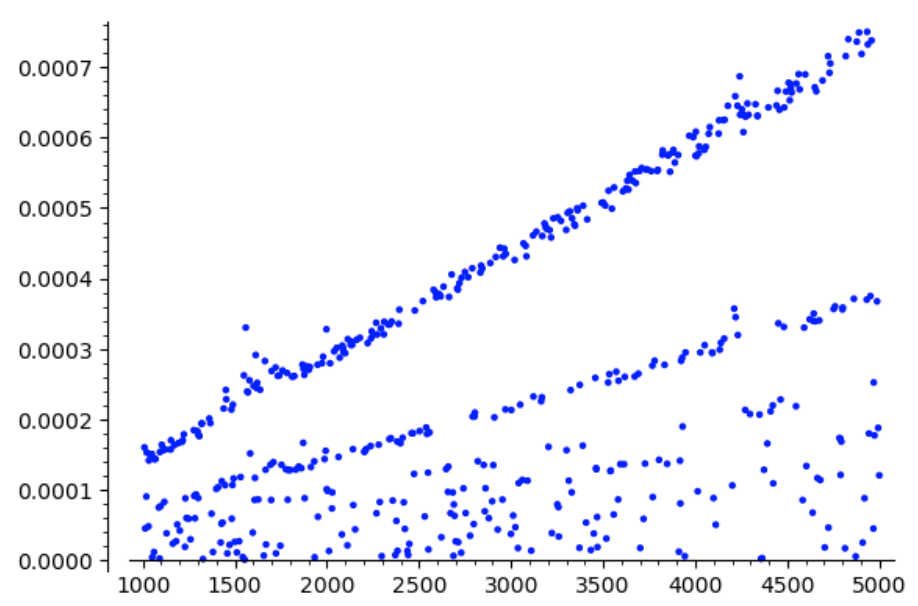
Умножение на число (возможно ускорение подобное быстрому возведению в степень):

N раз

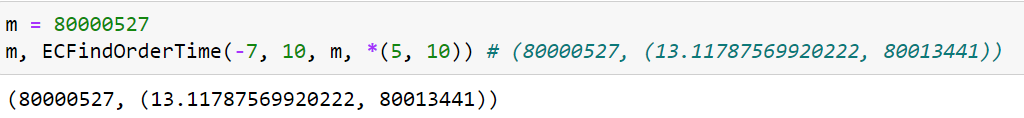
График эллиптической кривой с коэффициентами



Для решения поставленной задачи я выбрал коэффициенты , и решил проверить, как будет зависеть порядок точки от величины характеристики поля . График зависимости:



Видно, что порядок точки увеличивается как-то линейно. На основании этого факта можно было легко подобрать такое , при котором поиск порядка начальной точки будет около 10 минут. На моем оборудовании подошло значение .



Время поиска порядка точки составило чуть больше 13 минут.

Алгоритм поиска подразумевает постоянное суммирование аккумулятора с т. P, пока первый не станет нулем. Код:

1. **def** ECFindOrderTime(a, b, p, x0, y0):
2. p1 **=** Point(a, b, p, x0, y0)
4. i **=** 1
5. temp **=** p1
6. result **=** [(p1.x, p1.y)]
8. start **=** time.time()
9. **while** **not**(temp.x **==** temp.y **==** 0):
10. temp **+=** p1
11. i**+=**1
12. end **=** time.time()
14. **return** (end **-** start) **/** 60, i

**Выводы**

В ходе работы я познакомился с эллиптическими кривыми над конечными полями. Реализовал арифметические сложение точек и быстрое умножение на натуральное число, написал программу, определяющую порядок точки полным перебором. Ссылка на [GitHub](https://github.com/Igor743646/Krypt/blob/master/Lab2%20Kryptography.ipynb) с реализацией. Также существует алгоритм Шуфа, определения количества точек эллиптической кривой со сложность и метод комплексного умножения.