**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Московский Авиационный Институт»**

**(Национальный Исследовательский Университет)**

**Институт: №8 «Информационные технологии   
и прикладная математика»   
Кафедра: 806 «Вычислительная математика   
и программирование»**

Лабораторная работа № 5   
по курсу «Криптография»

Группа: М8О-307Б-21

Студент: Дубровин Д.К.

Преподаватель: А. В. Борисов

Оценка:

Дата: 16.09.2024

Москва, 2024

**ОГЛАВЛЕНИЕ**

[1 Тема 3](#_Toc158983147)

[2 Задание 3](#_Toc158983148)

[3 Теория 4](#_Toc158983149)

[4 Ход лабораторной работы 5](#_Toc158983150)

[5 Выводы 6](#_Toc158983151)

# **Тема**

Эллиптические кривые

# **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 .

# **Теория**

Эллиптические кривые – это особенный класс кривых, обладающих определёнными уникальными свойствами и играющих важную роль в различных областях математики и информационной безопасности. В самом общем виде, эллиптическая кривая определяется уравнением вида , где и являются константами, и для которых должно выполняться условие , чтобы исключить наличие особых точек, где кривая сама пересекает себя или имеет излом.

Эллиптические кривые обладают структурой абелевой группы, что означает возможность определения операций сложения и удвоения точек на кривой. Эти операции обладают свойствами ассоциативности, коммутативности, наличия нейтрального элемента (бесконечно удаленная точка) и обратного элемента.

На эллиптических кривых задача нахождения логарифма (т.е. решение уравнения вида , где - известная точка на кривой, - другая точка на кривой, а - неизвестный множитель) является вычислительно сложной, что лежит в основе их применения в криптографии.

Эллиптические кривые находят широкое применение в алгоритмах шифрования и цифровой подписи, таких как **ECDSA** (Elliptic Curve Digital Signature Algorithm) и **ECDH** (Elliptic Curve Diffie-Hellman). Они позволяют создавать более короткие ключи по сравнению с традиционными методами шифрования при сохранении аналогичного уровня безопасности. Эллиптические кривые также используются для изучения свойств чисел, в частности, в контексте Великой теоремы Ферма и задачи факторизации целых чисел.

**Что там про ?**

Поле , где — простое число, также известное как поле вычетов по модулю , представляет собой фундаментальный объект в алгебре, который находит широкое применение в теории чисел, криптографии, и других областях математики. Оно состоит из целых чисел от 0 до включительно, где арифметические операции (сложение, вычитание, умножение и деление) выполняются по модулю .

Свойства поля:

1. **Замкнутость**: Результат любой арифметической операции над элементами поля снова является элементом этого поля.
2. **Коммутативность**: Для всех операций коммутативно, т.е. порядок операндов не влияет на результат.
3. **Ассоциативность**: Группировка операндов не влияет на результат операции.
4. **Наличие нейтральных элементов**: 0 является нейтральным элементом для сложения, а 1 — для умножения.
5. **Наличие обратных элементов**: Для каждого элемента в существует обратный элемент такой, что .

используется в криптографических алгоритмах и протоколах, включая RSA, алгоритмы на эллиптических кривых и протоколы секретного обмена ключами. Поля вычетов применяются в теории кодирования для построения кодов, способных исправлять ошибки.

**Теоремы/алгоритмы для ускорения перебора**

Для ускорения нахождения точек на эллиптической кривой и избегания полного перебора можно использовать различные алгоритмы и теоремы:

1. **Сложение и удвоение точек на эллиптической кривой**

Сложение и удвоение точек на эллиптической кривой являются основными операциями, используемыми для генерации новых точек из уже известных. Эти операции обычно требуют фиксированного количества арифметических действий над элементами поля, поэтому их сложность можно считать константной для каждой операции.

Сложность: для каждой операции.

1. **Теорема Хассе**

Теорема Хассе дает верхнюю и нижнюю границы для количества точек на эллиптической кривой, что может быть полезно для оценки размера группы точек и проверки полноты набора найденных точек.

1. **Алгоритм Шуфа для поиска порядка точки**

Алгоритм Шуфа используется для нахождения порядка заданной точки на эллиптической кривой. Он эффективен для кривых над большими полями и использует понятие "делимости порядка" для ускорения поиска.

Сложность: От до , где — порядок группы точек.

1. **Алгоритмы факторизации и поиска порядка группы**

Эти алгоритмы используют идею случайного поиска для нахождения факторов числа или логарифмов в группе, что может быть применено для нахождения порядка группы точек на эллиптической кривой.

Алгоритм Полларда для факторизации: Сложность , где — число для факторизации.

Алгоритм Полларда для логарифмов: Сложность также примерно , где — размер группы.

1. **Алгоритм Сильвермана-Тейта**

Алгоритм Сильвермана-Тейта использует сложные алгебраические методы, включая теорию комплексного умножения и L-полиномы, для вычисления порядка группы точек эллиптической кривой.

# **Ход лабораторной работы**

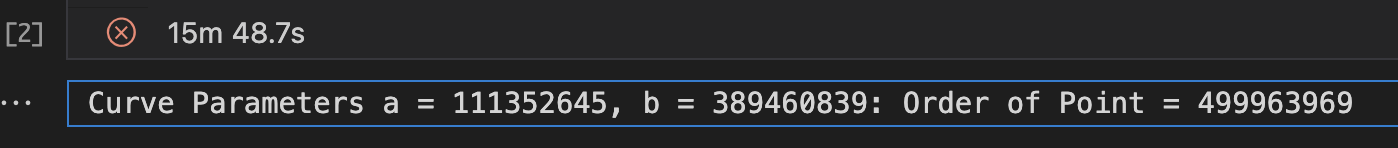
Я сначала оказывается делал не то задание, написал отчет и думал все. Потом я понял, что сделал не то. Начал делать то, что нужно, но никак не получалось. Мне помогла статья на хабре с лекции, так как там были моменты, которые я не учел. В течении часа я внес все правки и получил результат.

Curve Parameters:

a = 111352645;  
b = 389460839.

Order of Point = 499963969

Computation Time = 15 min 48 sec



Технические характеристики ноутбука:

|  |  |
| --- | --- |
| Операционная система | macOS Sonoma |
| Процессор | Apple M1 |
| Оперативная память | 8 ГБ |
| Экран | 13.3", 2560х1600 |
| Встроенная память | 256 Гб SSD |
| Ввод | Клавиатура macOS, Тачпад |
| Видеокарта | - |
| Bluetooth | Bluetooth 5.0 |
| Wi-Fi | Wi-Fi 6 (802.11ax) |
| Порты | 2 x USB Type-C  Mini jack |
| Звук | Dolby Atmos |
| Доп. устройства | Камера 1FaceTime 720p (HD), Светодиодная подсветка клавиатуры, TouchID |

# **Выводы**

Это была интересная заключительная лабораторная работа. Было интересно тыкать параметры, чтобы получить нужный результат. Да и было интересно узнать применение такой вещи как эллиптическая кривая.

# **Список используемой литературы**

1. <https://habr.com/ru/articles/335906/>