**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 № 4  
по курсу «Криптография»

Группа: М8О-307Б-22

Студент: Е. С. Кострюков

Преподаватель: А. В. Борисов

Оценка:

Дата: 24.04.2025

Москва, 2025

**ОГЛАВЛЕНИЕ**

[**Тема** 3](#_Toc196400961)

[**Задание** 3](#_Toc196400962)

[**Теория** 3](#_Toc196400963)

[**Ход лабораторной работы** 6](#_Toc196400964)

[**Выводы** 11](#_Toc196400965)

# **Тема**

Подбор эллиптической кривой с точкой, порядок которой находится полным перебором ~ за 10 минут

# **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.

# **Теория**

**Эллиптические кривые над конечным полем**

Эллиптические кривые находят широкое применение в современной криптографии благодаря высокой степени безопасности при относительно малых размерах ключей. Основой являются алгебраические структуры, задаваемые уравнением:

E: y2 ≡ x3 + ax + b (mod p)

где a, b ∈ Fp , p — простое число, а Fp — конечное поле из p элементов. Чтобы кривая была корректной (невырожденной), должно выполняться условие:

4a3 + 27b2 ≢ 0 (mod p)

Это условие исключает случаи, в которых уравнение описывает не кривую, а сингулярную (вырожденную) кривую с точками самопересечения или cusps.

**Операции над точками**

Точки, лежащие на эллиптической кривой, вместе с точкой на бесконечности O, образуют абелеву группу. Основные операции в этой группе:

* Сложение точек: геометрически интерпретируется как нахождение третьей точки пересечения прямой с кривой.
* Удвоение точки: приближение касательной к кривой в данной точке и аналогичное нахождение третьей точки пересечения.

Алгебраически операции реализуются с помощью формул, зависящих от координат точек и параметров a, p.

**Порядок точки**

Порядком точки P называется наименьшее положительное целое число n, такое что nP = O, где O — нейтральный элемент (аналог нуля в аддитивной группе).

Для вычисления порядка можно использовать:

* Полный перебор — самый простой, но медленный метод, заключающийся в последовательном сложении точки с собой, пока результат не станет равен O.
* Теорема Лагранжа — порядок любой точки делит порядок всей группы точек на кривой.
* Теорема Хассе — даёт границы на количество точек на кривой:

∣E(Fp) − (p + 1)∣ ≤ 2p1/2 .

**Методы ускорения вычисления порядка точки на эллиптической кривой**

Хотя полный перебор — простой и универсальный метод нахождения порядка точки на эллиптической кривой, его временная сложность составляет O(n), где n — искомый порядок. На практике это может быть крайне неэффективно при больших значениях порядка. Для ускорения этой задачи разработаны теоремы и алгоритмы, позволяющие значительно сократить время вычислений.

**Теорема Лагранжа**

Если точка P лежит на эллиптической кривой над полем Fp, то её порядок n делит порядок группы E(Fp). То есть:

n ∣ E(Fp)n

Таким образом, если заранее известно (или вычислено) количество точек на кривой, можно ограничить перебор делителями этого числа, что уже значительно ускоряет процесс.

**Теорема Хассе**

Оценка Хассе даёт границы на возможное число точек на эллиптической кривой:

∣E(Fp) − (p + 1)∣ ≤ 2p1/2

Следовательно, E(Fp) ∈ [p + 1 − 2p1/2, p + 1 + 2p1/2]. Это позволяет сужать диапазон перебора возможного порядка и использовать его делители.

**Алгоритм Бэби-степ — Джайнт-степ (BSGS)**

Один из классических методов для нахождения порядка точки и дискретного логарифма. Идея основана на хранении промежуточных результатов и последующем поиске совпадения. Сложность метода — O(n1/2) как по времени, так и по памяти.

Принцип:

1. Выбирается m=⌈n1/2⌉.
2. Вычисляются и запоминаются значения jP для j = 0, 1, ..., m − 1.
3. Затем считаются Q − i(mP) и проверяется совпадение.

Этот алгоритм в 1000 и более раз быстрее полного перебора при достаточно больших значениях порядка, но требует памяти O(n1/2).

**Алгоритм Полларда «ρ» для эллиптических кривых**

Это вероятностный алгоритм для нахождения дискретного логарифма, но может быть адаптирован для поиска порядка точки. В основе метода лежит идея случайного блуждания и выявления коллизии.

Преимущества:

* Не требует большого объема памяти (в отличие от BSGS);
* В среднем работает за O(n1/2) операций.

Принцип: строится псевдослучайная последовательность точек и используется идея цикла (аналогично алгоритму Флойда для поиска цикла в списке).

**Использование делителей предполагаемого порядка**

Если предварительно вычислить (или оценить) порядок группы точек на кривой, то можно заранее разложить его на множители и проверять только эти делители. Это особенно эффективно, если порядок — составное число с малыми простыми делителями.

**Методы на основе структуры группы**

Некоторые эллиптические кривые (например, кривые с заданной структурой группы) позволяют сразу определять порядок группы или даже точек. Пример — кривые с коразделённой группой, двойные кривые, GLV-методы и др.

**Предварительная оптимизация кода**

Даже при использовании полного перебора можно значительно ускорить вычисления за счёт:

* оптимизации операций сложения/удвоения (например, использование аффинных или проективных координат),
* компиляции кода (например, Cython или Numba),
* распараллеливания (многопоточность).

# **Ход лабораторной работы**

**Цель**

Подобрать такие параметры эллиптической кривой и точку на ней, чтобы полный перебор порядка точки занимал около 10 минут на заданном вычислителе.

**Используемые инструменты**

Для выполнения лабораторной работы использовался язык программирования Python 3.12 и библиотеки:

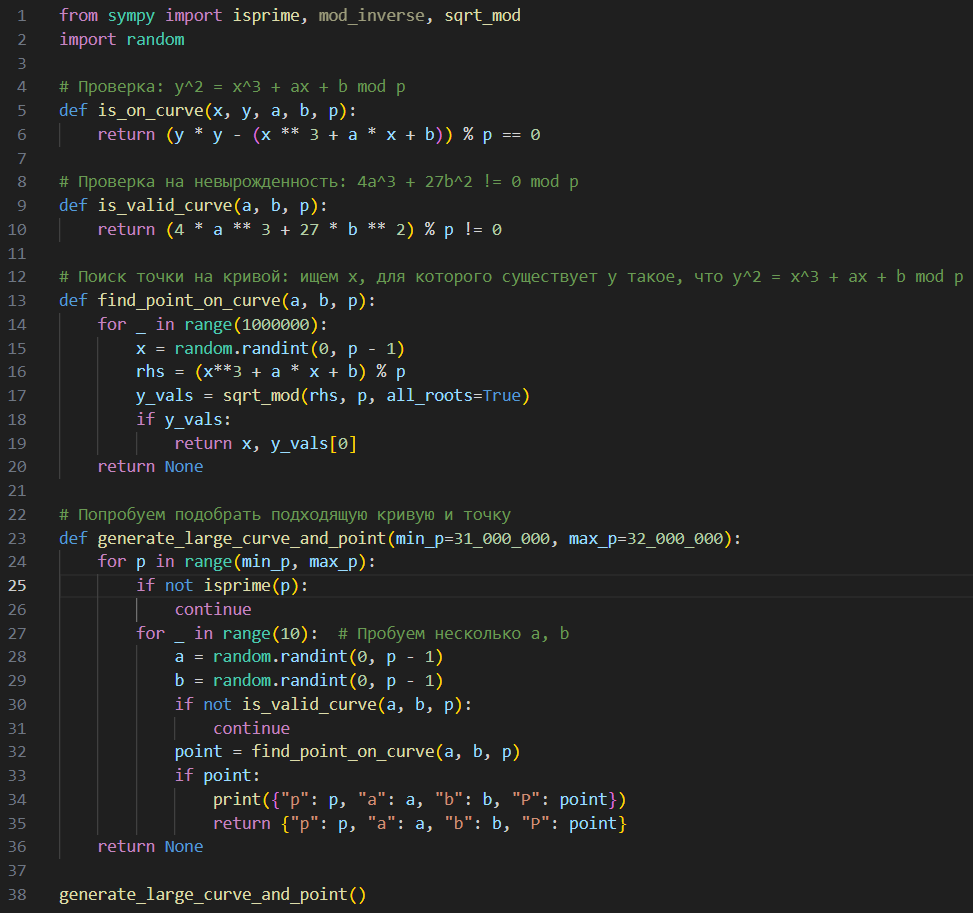
* sympy для работы с модулярной арифметикой и проверки условий на кривую;
* cpuinfo, platform для сбора характеристик системы;
* встроенные функции Python для генерации случайных чисел и измерения времени.

**Подбор кривой**

В первом скрипте осуществляется:

* выбор простого числа p в заданном диапазоне;
* генерация параметров a и b и проверка невырожденности;
* поиск точки на кривой путём генерации случайного x и нахождения квадрата по модулю p, равного x3 + ax + b.

**Исходный код:**

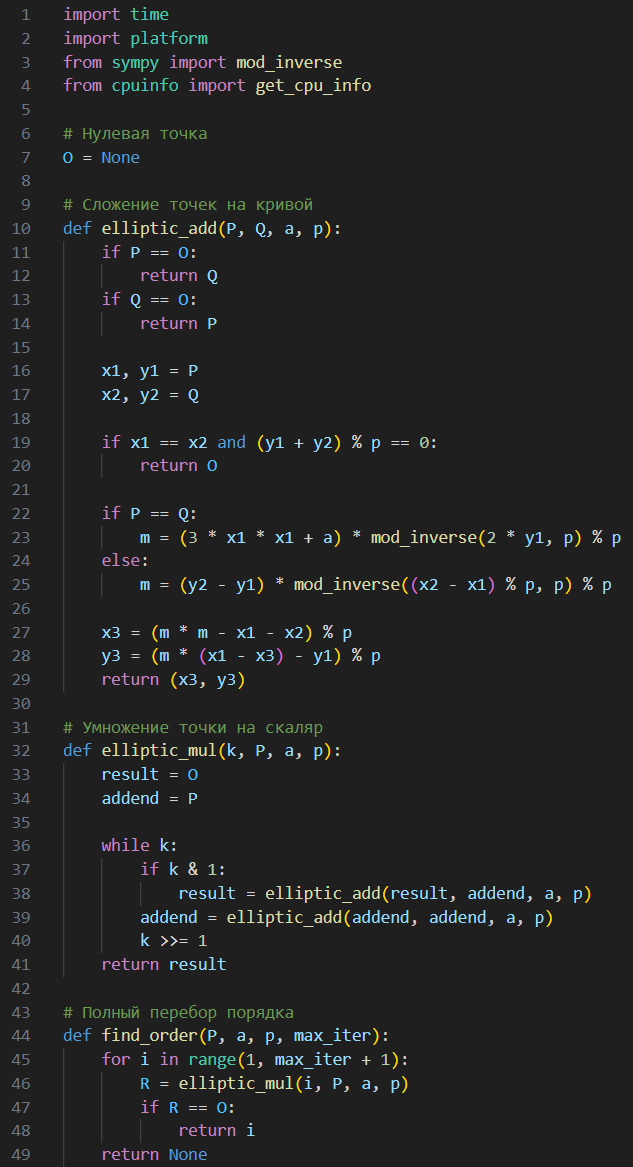


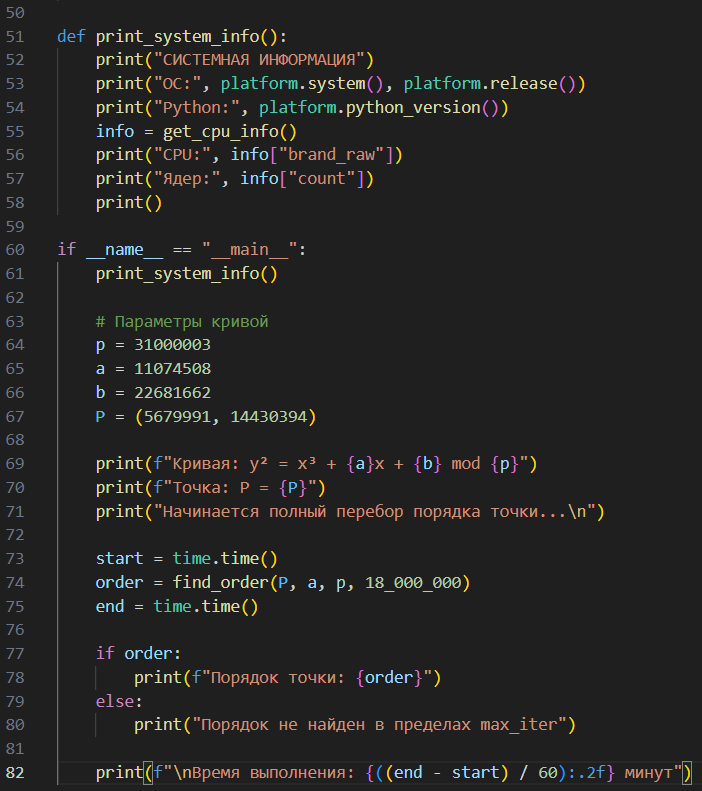
**Результат выполнения:**



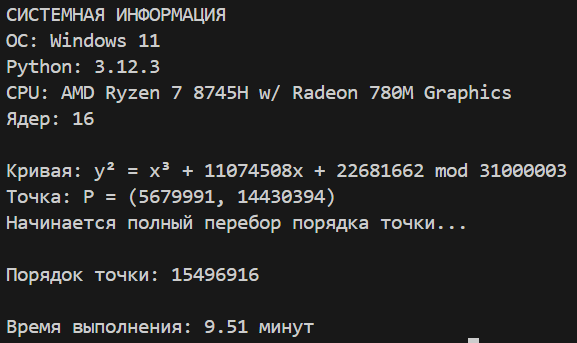
**Поиск порядка**

Во втором скрипте реализован алгоритм полного перебора: итеративное умножение точки P на скаляр до тех пор, пока результат не станет равен O.

**Исходный код:**  




**Результат выполнения:**



# **Выводы**

1. Был успешно реализован подбор эллиптической кривой и точки на ней, соответствующей требованию: нахождение порядка методом полного перебора за время около 10 минут.
2. Продемонстрирована практическая реализация операций на эллиптической кривой в поле Fp.
3. Получены навыки работы с криптографическими примитивами и их реализацией на практике.
4. Исследованы алгоритмы оптимизации вычислений порядка точки, включая теоремы и методы, применяемые в реальных криптографических протоколах.
5. Вычисления подтвердили корректность реализованных алгоритмов и подобранных параметров.