МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра дифференциальных уравнений и системного анализа

АНАЛИЗ ЭФФЕКТИВНОСТИ ВЫЧИСЛЕНИЯ ОПЕРАЦИИ СЛОЖЕНИЯ ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ ПРИ ПОМОЩИ ПРОЕКТИВНЫХ КООРДИНАТ

Подготовила студентка 2-го курса
Шклярик Вера Сергеевна

Научный руководитель:
кандидат физ.-мат. наук,
доцент Д. Н. Чергинец

Минск, 2023

Постановка цели

Цель: Провести анализ эффективности вычисления операции сложения точек эллиптической кривой при помощи проективных координат, координат Якоби, обобщенных координат Якоби.
Задачи:

- Изучить понятие эллиптической кривой, правила сложения точек на эллиптической кривой.
- Провести вывод формул сложения точек эллиптической кривой в конечном поле порядка p, p – простое, p>3, в аффинных координатах, в проективных координатах, координатах Якоби, обобщенных координатах Якоби.
- Реализовать в Python алгоритмы сложения точек эллиптической кривой в рассматриваемых системах координат.
- Провести теоретический анализ эффективности изучаемых алгоритмов.
- Провести практический анализ эффективности изучаемых алгоритмов.

Область исследования

Эллиптической кривой над полем K в аффинной системе координат называется множество точек $(x, y) \in K^2$, удовлетворяющих уравнению:

$$y^2 = x^3 + ax + b,$$

где $a, b \in K$.

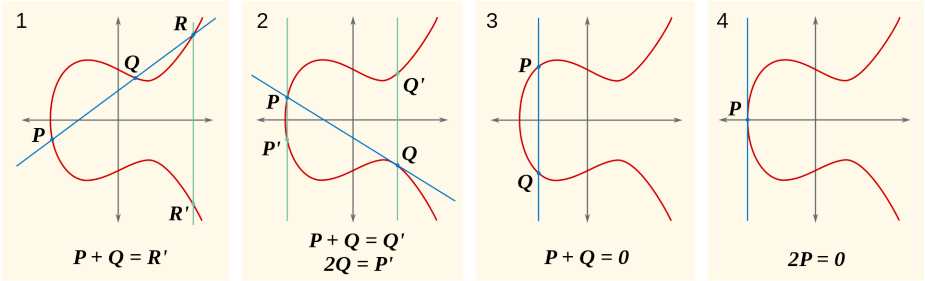

Рис. 1: Сложение точек эллиптической кривой геометрически.
1, 3 - сложение различных точек, 2, 4 - удвоение точки.

Системы координат

Время выполнения операции сложения в различных системах координат

```
Аффинные координаты:--- 20.042898654937744 seconds ---
Проективные координаты:--- 10.82426643371582 seconds ---
Координаты Якоби:--- 9.010782241821289 seconds ---
Обобщенные координаты Якоби:--- 8.495838403701782 seconds ---
```

Вывод формул. Аффинные и проективные координаты

Сумма точек $P = (x_1, y_1)$ и $Q = (x_2, y_2)$ в аффинных координатах:

$$\left(\left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2, - \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^3 + x_2 \frac{y_2 - y_1}{x_2 - x_1} - y_1 \right)$$

В проективных координатах сумма $P = (X_1, Y_1, Z_1)$ и $Q = (X_2, Y_2, Z_2)$ имеет вид

$$(\frac{w}{v^2 Z_1 Z_2}, \frac{u(v^2 X_1 Z_2 - w) - v^3 Y_1 Z_2}{v^3 Z_1 Z_2}, 1)$$

Чтобы избежать деления, выберем другого представителя данной проективной точки:

$$(vw, u(v^2 v_2 - w) - v^3 u_2, v^3 Z_1 Z_2),$$

где $u = Y_2 Z_1 - Y_1 Z_2, \quad v_2 = X_1 Z_2, \quad v = X_2 Z_1 - v_2, \quad w = u^2 Z_1 Z_2 - v^3 - 2v^2 v_2.$

Реализация

класс Точка
(Point, ProjectivePoint, JacobianPoint, ChudnovskyJacobianPoint)

- Сложение (оператор `+`)
- Умножение (`*`)
- Вычитание (`-`)
- Сравнение (`==`)
- Перевод между системами координат

класс Кривая
(Curve, ProjectiveCurve, JacobianCurve, ChudnovskyJacobianCurve)

- Поиск всех точек кривой
- Генерация случайной точки кривой
- Принадлежность точки кривой
- Сравнение (`==`)
- Перевод между системами координат

Теоретический анализ

I - операция вычисления обратного элемента, M - умножение различных чисел, S - возведение числа в квадрат.

Количество арифметических операций		
Система координат	Удвоение точки	Сложение различных точек
Аффинные координаты	$I + 2M + 2S$	$I + 2M + S$
Проективные координаты	$12M + 5S$	$21M + 2S$
Координаты Якоби	$10M + 7S$	$18M + 4S$
Обобщенные координаты Якоби	$9M + 6S$	$16M + 3S$

Таблица 1: Количество арифметических операций, выполняемых алгоритмами сложения и удвоения в различных системах координат

Практический анализ

Тесты проводились на эллиптической кривой SECP256k1, которая рассматривается над полем порядка $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$.

```
Аффинные координаты:----------- 3.729386806488037 seconds ----
Проективные координаты:-------- 1.835113763809204 seconds ----
Координаты Якоби:-------------- 1.5577855110168457 seconds ---
Обобщенные координаты Якоби:--- 1.3425955772399902 seconds ---
```

Можно утверждать, что переход от аффинной системы координат к проективным координатам, координатам Якоби и обобщенным координатам Якоби целесообразен, ведь в любой из данных систем координат сложение выполняется значительно быстрее.

Результаты

В ходе работы:

- Описан предмет исследования, эллиптическую кривую, а также процесс сложения точек на эллиптической кривой с геометрической точки зрения.
- Проведен подробный вывод формул сложения и удвоения точек эллиптической кривой в аффинных координатах, проективных координатах, координатах Якоби, обобщенных координатах Якоби.
- Реализованы алгоритмы сложения точек эллиптической кривой в конечном поле в рассматриваемых системах координат на языке Python.
- Проведен теоретический анализ эффективности изучаемых алгоритмов.
- Проведен практический анализ эффективности изучаемых алгоритмов.