МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра дифференциальных уравнений и системного анализа

ОТЧЕТ О ПРОХОЖДЕНИИ ВЫЧИСЛИТЕЛЬНОЙ ПРАКТИКИ

Студентка группы 5, 2 курса, специальности
1-31 03 09 Компьютерная математика
и системный анализ В.С. Шклярик

Руководитель практики от кафедры Д.Н. Чергинец

Минск 2023

ОГЛАВЛЕНИЕ

ЗАДАНИЕ НА ВЫЧИСЛИТЕЛЬНУЮ ПРАКТИКУ

Тема: Эндоморфизмы эллиптических кривых и проблема дискретного логарифма

Содержание работы:

1. Эллиптическая кривая в форме Вейерштрасса;
2. Эндоморфизмы эллиптических кривых;
3. Эффективно вычисляемые эндоморфизмы эллиптических кривых;
4. Эллиптические кривые при $a = 0, b = 7$ и $p \equiv 1 \pmod 3$ с простым порядком n
   - Всегда ли $n \equiv 1 \pmod 3$?
   - Решение уравнения $xG = P_1$ по известному решению уравнения $xG = P_2$, где P_1 и P_2 имеют одинаковую координату y.
   - Решение уравнения $xG = P_1$ по известному решению уравнения $xG = P_2 - P_1$, где P_1 и P_2 имеют одинаковую координату y.
   - Поиск других свойств данной кривой.
5. Реализация изученных алгоритмов в Python.

ВВЕДЕНИЕ

Данная исследовательская работа посвящена анализу эффективно вычисляемых эндоморфизмов эллиптических кривых и их применению в решении проблемы дискретного логарифма.

Целью работы является решение в частном случае задачи поиска дискретного логарифма на эллиптических кривых вида $y^2 = x^3 + 7$ с простым порядком n с помощью эффективно вычисляемых эндоморфизмов.

В рамках вычислительной практики мной были изучены понятия эллиптической кривой в конечном поле, эллиптической кривой в форме Вейерштрасса, понятие дискретного логарифма на эллиптической кривой. Я изучила понятие эндоморфизма эллиптических кривых, рассмотрела некоторые примеры эффективно вычисляемых эндоморфизмов. Для эллиптических кривых вида $y^2 = x^3 + 7$ с простым порядком n решены поставленные задачи:

- Всегда ли $n \equiv 1 \pmod 3$?
- Поиск решения уравнения $xG = P_1$ по известному решению уравнения $xG = P_2$, где P_1 и P_2 имеют одинаковую координату y.
- Поиск решения уравнения $xG = P_1$ по известному решению уравнения $xG = P_2 - P_1$, где P_1 и P_2 имеют одинаковую координату y.

Кроме того, я реализовала в Python алгоритмы решения рассматриваемых задач поиска дискретного логарифма и протестировала корректность их работы как на кривых малого порядка, так и на эллиптической кривой SECP256k1, которая используется в протоколах системы Bitcoin.

ОСНОВНАЯ ЧАСТЬ ОТЧЕТА

Выполняемое мной задание можно разделить на теоретическую часть, в которой я изучала необходимый для решения поставленных задач материал, а затем решала задачи непосредственно математически, и практическую часть, в которой я реализовывала алгоритмы решения задач поиска дискретного логарифма, а затем тестировала их корректность. В основной части отчета мной будут приведены как необходимые теоретические сведения, касающиеся моего исследования, так и описание выполненной работы по разделам индивидуального задания.

Эллиптическая кривая в форме Вейерштрасса

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

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

где $a_i \in K$. Такая кривая должна быть неособой в том смысле, что частные производные функции $F = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$ по переменным x, y не должны обращаться в нуль одновременно ни в одной точке кривой. Кроме того, к эллиптической кривой добавляют бесконечно удаленную точку O. Уравнение (1) называется длинной формой уравнения Вейерштрасса.
Для эллиптической кривой E вводятся следующие константы:

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2,\\
b_4 &= a_1a_3 + 2a_4,\\
b_6 &= a_3^2 + 4a_6,\\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_4^2,\\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,
\end{aligned}$$

где число Δ называют дискриминантом кривой E. Кривая неособа тогда и только тогда, когда $\Delta \neq 0$, что мы и будем полагать далее. В конечном поле простого порядка p, p $>$ 3 допускается замена переменных

$$x = x' - \frac{b_2}{12},$$
$$y = y' - \frac{a_1}{2}(x' - \frac{b_2}{12}) - \frac{a_3}{2},$$

переводящая кривую E', заданную уравнением (1) в изоморфную ей кривую E, определяемую следующим уравнением (короткая или нормальная форма Вейерштрасса):

$$y^2 = x^3 + ax + b \tag{2}$$

при некоторых $a, b \in K$. Дискриминант такой кривой равен $-16(4a^3 + 25b^2)$. [1, с. 55]. На эллиптической кривой вводятся операции сложения точек и умножения точки на скаляр. Отметим также, что точки эллиптической кривой образуют аддитивную абелеву группу.

Эндоморфизмы эллиптических кривых

Эндоморфизмом эллиптической кривой E называется рациональное отображение $\phi : E \to E$, для которого $\phi(O) = O$. Эндоморфизм E также является гомоморфизмом абелевой группы точек кривой E. [2]

Эффективно вычисляемые эндоморфизмы эллиптических кривых

Рассмотрим некоторые примеры эффективно вычисляемых эндоморфизмов эллиптических кривых.

Пример 1. Пусть E - эллиптическая кривая над полем $\mathbb{F}_p$. Для каждого $m \in \mathbb{Z}$ умножение на число m $[m] : P \mapsto mP$ является эндоморфизмом над полем $\mathbb{F}_p$. Частным случаем является отображение $P \mapsto -P$.

Пример 2. Пусть снова E - эллиптическая кривая над полем $\mathbb{F}_p$. Тогда возведение в q степень $\phi : E \to E$, $(x, y) \mapsto (x^p, y^p)$ и $\mathcal{O} \mapsto \mathcal{O}$ является эндоморфизмом, называемым эндоморфизмом Фробениуса. Поскольку возведение в степень по простому модулю p выполняется с помощью линейного алгоритма быстрого возведения в степень, вычисление $\phi(P)$ можно считать эффективным.

Пример 3. Пусть $p \equiv 1 \pmod 4$ - простое число. Рассмотрим эллиптическую кривую

$$E_1 : y^2 = x^3 + ax,$$

определенную над полем $\mathbb{F}_p$. Пусть $\alpha \in \mathbb{F}_p$ - элемент порядка 4. Тогда отображение $\phi : (x, y) \mapsto (-x, \alpha y)$ и $\mathcal{O} \mapsto \mathcal{O}$ - эндоморфизм над полем $\mathbb{F}_p$. Если $P \in E(\mathbb{F}_p)$ - точка простого порядка n, тогда ϕ действует на $\langle P \rangle$ как оператор умножения $[\lambda]$, т.е., $\phi(Q) = \lambda Q$ для всех $Q \in \langle P \rangle$, где $\lambda \in \mathbb{Z}$ удовлетворяет $\lambda^2 \equiv -1 \pmod n$. Заметим, что $\phi(Q)$ можно вычислить с помощью одной операции умножения в $\mathbb{F}_p$.

Пример 4. Пусть $p \equiv 1 \pmod 3$ - простое. Рассмотрим эллиптическую кривую

$$E_2 : y^2 = x^3 + b$$

над полем $\mathbb{F}_p$. Пусть $\beta \in \mathbb{F}_p$ - элемент порядка 3. Тогда отображение $\phi : (x, y) \mapsto (\beta x, y)$ и $\mathcal{O} \mapsto \mathcal{O}$ есть эндоморфизм над полем $\mathbb{F}_p$. Если $P \in E(\mathbb{F}_p)$ точка простого порядка n, тогда ϕ действует на $\langle P \rangle$ как оператор умножения $[\lambda]$, где $\lambda \in \mathbb{Z}$ удовлетворяет характеристическому уравнению $\lambda^2 + \lambda \equiv -1 \pmod n$. Заметим, что $\phi(Q)$ также можно можно вычислить с помощью единственной операции умножения. [2, с. 3]

Дискретное логарифмирование на эллиптической кривой

Пусть p — простое число, a, b — целые числа, отличные от нуля по модулю p. Предположим, что существует целое число k такое, что

$$a^k \equiv b \pmod p$$

Классическая задача дискретного логарифмирования состоит в том, чтобы найти k. В более общем случае пусть G будет группой и пусть $a, b \in G$. Предположим, мы знаем, что $a^k = b$ для некоторого целого числа k. В этом контексте задача дискретного логарифмирования снова состоит в том, чтобы найти k. Кроме того, G может быть группой точек эллиптической кривой $E(\mathbb{F}_p)$, и в этом случае A и B являются точками на E, и мы должны найти целое число k, такое, что $kA = B$.

Эллиптические кривые при $a = 0$, $b = 7$ и $p \equiv 1 \pmod 3$ с простым порядком n

Областью моего исследования являются эллиптические кривые вида $y^2 = x^3 + 7$ над полем полем простого порядка p, для которых порядок кривой n - также простое число. Ответим вначале на вопрос о порядке данной кривой, а именно, всегда ли $n \equiv 1 \pmod 3$? Воспользуемся следующей теоремой [3, с. 6]:

Теорема 1. *Пусть $p \equiv 1 \pmod 3$ - простое число и пусть $E(\mathbb{F}_p) : y^2 = x^3 + B$ - эллиптическая кривая. Тогда для порядка n справедливо:*

$$n = \begin{cases} p + 1 + 2a & B \text{ вычет шестой степени по модулю } p, \\ p + 1 - 2a & B \text{ кубический, но не квадратичный вычет по модулю } p, \\ p + 1 - a \pm 3b & B \text{ квадратический, но не кубический вычет по модулю } p, \\ p + 1 + a \pm 3b & B \text{ не является квадратическим или кубическим вычетом} \end{cases}$$

где $p = a^2 + 3b^2$, $b > 0$, и $a \equiv 2 \pmod 3$.

Последовательно вычисляя остатки от деления n на 3 в каждом из случаев, получим, что если $B = 7$ является квадратическим вычетом или вычетом шестой степени, то порядок n делится на 3, то есть n не является простым числом, что не соответствует рассматриваемым в данной работе кривым, а если $B = 7$ является кубическим вычетом или же вовсе не является вычетом 2 или 3 степени, то $n \equiv 1 \pmod 3$.

Для решения поставленных задач, связанных с вычислением дискретного логарифма на рассматриваемой кривой следует воспользоваться свойствами эндоморфизма, ранее описанного в Примере 4. Кроме того, поскольку $n \equiv 1 \pmod 3$, а эндоморфизм использует константу β порядка 3, то получаем, что множество точек кривой разбивается на тройки точек с одинаковой координатой y. Это найденное мной свойство рассматриваемой кривой в сущности позволяет решить поставленные задачи поиска дискретного логарифма. Для характеристического уравнения $\lambda^2 + \lambda \equiv -1$ верно

$$\lambda^3 \equiv -\lambda(\lambda + 1) \equiv -\lambda^2 - \lambda \equiv 1 \pmod n,$$

то есть λ является элементом порядка 3 в поле $\mathbb{F}_p$.

Теперь опишем алгоритм решения первой задачи: решить уравнение $xG = P_1$ по известному решению уравнения $xG = P_2$, где P_1 и P_2 имеют одинаковую координату y. Пусть $P_2 = tG$. Поскольку точки P_1, P_2 имеют одинаковую координату y, а множество точек кривой разбивается на тройки, то существует также третья точка P_3 с той же ординатой. Применяя эндоморфизм $\phi : (x, y) \mapsto (\beta x, y)$ к точке P_1 получим либо известную нам точку P_2, либо точку P_3. Если в результате точка P_1 перешла в P_2, то получаем

$$\lambda P_1 = P_2 = tG \Rightarrow \lambda x G = tG \Rightarrow x = t\lambda^{-1} \pmod n$$

Если же точка P_1 перешла в P_3, то

$$\lambda P_1 = P_3,\ \lambda P_3 = P_2 = tG \Rightarrow \lambda^2 P_1 = tG \Rightarrow \lambda^2 x G = tG \Rightarrow x = t\lambda^{-2} \pmod n$$

Для реализации данного алгоритма необходимо лишь вычислить β, λ как нетривиальные кубические корни из 1 по модулям p, n соответственно.

Перейдем ко второй из рассматриваемых задач: решить уравнение $xG = P_1$ по известному решению уравнения $xG = P_2 - P_1$, где P_1 и P_2 имеют одинаковую координату y. Если применяя эндоморфизм к P_1 мы получили точку P_2, то дискретный логарифм вычисляется следующим образом:

$$tG = P_2 - P_1 = \lambda P_1 - P_1 = \lambda x G - xG \Rightarrow$$
$$\Rightarrow t = \lambda x - x = x(\lambda - 1) \Rightarrow$$
$$\Rightarrow x = t(\lambda - 1)^{-1} \pmod n$$

Если же точка P_1 перешла в P_3, то

$$x = t(\lambda^2 - 1)^{-1} \pmod n$$

Реализация алгоритмов в Python

Таким образом, я вывела математические алгоритмы решения поставленных задач поиска дискретного логарифма, после чего реализовала данные алгоритмы на языке Python, в среде Jupyter Notebook. Для реализации мне потребовались классы Curve и Point, описывающие эллиптическую кривую и точку эллиптической кривой соответственно. Данные классы были реализованы мной ранее в курсовой работе. Кроме того, я использовала функцию `nthroot_mod` из модуля `ntheory.residue_ntheory` библиотеки `sympy` для вычисления нетривиальных корней из единицы по простому модулю, поскольку встроенная функция `pow` возвращает лишь единственный тривиальный корень 1, который не подходит для дальнейших вычислений. Корректность работы реализованных алгоритмов я тестировала как на кривой малого порядка $p = 43,\ n = 31$, так и на кривой SECP256k1, для который как модуль $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$, так и порядок кривой n являются числами порядка 256. В обоих случаях алгоритмы возвращали правильные ответы, а проводимые тесты приведены в приложении к отчету. Анализ скорости выполнения вычислений, а также сравнение с существующими алгоритмами вычисления дискретного логарифма на эллиптических кривых, на мой взгляд, не имеет смысла, поскольку в данной работе рассматривается задача поиска дискретного логарифма лишь для частного вида эллиптической кривой, и каждый из описанных мной алгоритмов выполняет не более десяти арифметических операций, что обеспечивает несравнимо большую скорость, чем существующие алгоритмы вычисления дискретного логарифма в общем случае.

ЗАКЛЮЧЕНИЕ

В ходе прохождения вычислительной практики я приобрела как практические навыки, так и теоретические знания в сфере криптографии, а именно в области эллиптических кривых и проблемы дискретного логарифма. В ходе моего исследования я познакомилась с понятием эндоморфизма эллиптических кривых и изучила некоторые примеры эффективно вычисляемых эндоморфизмов. Решая поставленные передо мной задачи, я вывела ряд свойств эллиптической кривой вида $y^2 = x^3 + 7$, что позволило мне получить алгоритм для решения задачи дискретного логарифма в некоторых частных случаях. Кроме того, алгоритмы поиска дискретного логарифма были реализованы и протестированы на различных кривых, включая кривую SECP256k1, используемую в протоколах системы Bitcoin. Реализация алгоритмов была выполнена на языке программирования Python.

В заключение хотелось бы отметить, что данная практика была очень полезной и позволила мне расширить свои знания и навыки в области криптографии. На основе полученного опыта, я планирую дальнейшее изучение и исследование данной тематики с целью применения этих знаний в различных областях информационной безопасности и криптографии.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] Смарт, Н. Криптография / Н. Смарт ; пер. с англ. С. А. Кулешова под ред. С. К. Ландо. - Москва : Техносфера, 2006.

[2] Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms [Электронный ресурс]–
Режим доступа: https://www.iacr.org/archive/crypto2001/21390189.pdf

[3] On Orders of Elliptic Curves over Finite Fields, Rose-Hulman Undergraduate Mathematics Journal [Электронный ресурс]–
Режим доступа: https://paperity.org/p/162644881/on-orders-of-elliptic-curves-over-finite-fields

[4] A survey of elliptic curves for proof systems by Diego F. Aranha, Youssef El Housni, Aurore Guillevic [Электронный ресурс]–
Режим доступа: https://inria.hal.science/hal-03667798/document

ПРИЛОЖЕНИЕ

Режим доступа: https://github.com/ksprski/practice2023