ЛАБОРАТОРНАЯ РАБОТА №5

АЛГОРИТМ ШУФА

ЦЕЛЬ РАБОТЫ: приобретение практических навыков в моделировании работы протоколов на эллиптических кривых.

**Введение**

Алгоритм Шуфа — эффективный алгоритм подсчёта числа точек на эллиптической кривой над конечным полем. Алгоритм имеет приложения в эллиптической криптографии, где важно знать число точек, чтобы судить о трудности решения задачи дискретного логарифмирования на группе точек на эллиптической кривой.

**Эндоморфизм Фробениуса**

Эндоморфизм Фробениуса расширяет эллиптическую кривую отображением (.

Идея Шуфа заключается в выполнении вычислений, ограничиваясь точками порядка *l* для различных малых простых чисел *l*. Если точка (x,y) находится в подгруппе кручения *l* расширенной эллиптической кривой , то , где P является точкой расширенной эллиптической кривой, является единственным целым числом, таким, что .

Если то . Задача сводится к решению уравнения (, где и лежат в интервале .

**Вычисления по простому модулю**

Многочлен деления с номером *l* это такой многочлен, что его корни являются в точности x координатами точек порядка *l*. Тогда ограничение вычисления (на точки *l*-кручения означает вычисление этих выражений как функций координатного кольца E и модуля *l*-го многочлена деления.

**Примечание:** Все дествия с многочленами производятся по модулю харакетристики эллептической кривой p (модулю простого числа эллептической кривой)

Многочлен деления рекурсивно определяется по следующим формулам:

-8

Для :

Для :

**Зачечания:** Так как не удобно работать с многочленами из двух переменных, то следует заменять на . Таким образом содержит только переменные по модулю x, если i – нечётно. И содержит единственное умножение на y при чётном i. Таким образом лучше ввести вспомогательный многочлен, который содержит только переменную x:

Тогда рекурсия для выглядит так:

Для :

Для :

С помощью многочленов деления можно эффективно вычислять склаярное умножения на точку элептической кривой в общем виде, по следующей формуле:

(, где – n-й многочлен деления.

**Зачечание:** Формулу выше можно записать используя вспомогательную функцию следующим образом:

(

Заметим, что в таком случае координата зависит только от x, и тоже хависит только от x

Выделяют два случая:

1. (

Используя формулу сложения для группы , мы получим:

X(x,y)= . Вычисление не выполняется в случае если предположение о неравентсве было неверно.

**Замечание:** данную формулу можно переписать, используя только значения x, заменив на :

X(x) =

1. (

Делается предположение, что , где q является квадратом по модулю *l*. Если выполняется условие , то . Если q не являетсяквадратом по модулю *l* или равенство не выполняется для некоторого w и -w, то наше предположение неверно так как и

**Алгоритм Шуфа**

Пусть дана эллиптическая кривая в короткой форме Вейерштрасса, где , , p -простое, n – целое .

1. Выбирается множество небольших простых чисел S, :
2. Пусть , если НОД(иначе
3. Для всех выполянем:
   1. Найдём - целое такое, что и
      1. Вычисляем многочлен деления (Далее все вычисления в алгоритме производятся по модулю многочлена , для вычисления координат точек в том числе)
      2. Вычисляем точки
   2. Если НОД(, то результат может быть не предсказуем и лучше выбрать за место этого значения *l* другое
   3. Если то:
      1. Вычисляем значения
      2. Для выполняем:
         1. Вычисляем
         2. Если то:
            1. Если то:
            2. то:
   4. Если q является квадратичным вычетом по *l* то:
      1. Вычисляем w, где
      2. Вычисляем
      3. Если то:
      4. Если то:
      5. Иначе
   5. Иначе

4. По КТО решаем систему уравнений и находим где

5. Выводим – число точек кривой E над .

**Пример вычисления**

Пусть дана эллиптическая кривая .

Тогда для определения порядка кривой мы имеем . Наша задача найти t:

Решение системы: . Для мы имеем t = -7.

Для l=2 вычисляем:

НОД(-x, =НОД(

не имеет корней в поле , так

Для l=3 вычисляем:

Выполняем теже действия и добиваемся, что j=1. Мы имеем и . Далее проверяем. Многочлен деления для l=3 равняется .

Вычисляем x координату

.

НОД(то есть мультипликативного обратного не существует. Поскольку x=8 является корнем , точка (8,4) будет иметь порядок 3. Следовательно , так

Для l=5 вычисляем:

Выполняем теже действия и добиваемся, что j=2. Обратим внимание, что Проверим есть ли , . Полином деления равен + 8.

Вычисляем:

Когда изменяется на , это приводит к полиномиальному соотношению в x, которое замтем проверяется. Следовательно,

Для определения знака смотрим на координату y. Координата y из , вычисляется как

Следует: из

Получаем . Это значит, что и следует, что

Решение системы уравнений даёт t=-7. И следует, что порядок кривой имеет 27 точек.

**Рабочее задание**

Написать программу, реализующую данный алгоритм.

Эллиптическая кривая получается генератором из лабораторной работы №3. На экран выводится сама кривая и количество её точек.