МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**«Исследование криптографических алгоритмов на основе эллиптических кривых. Задание №1.»**

Студент:

Септилко Анастасия Антоновна

Преподаватель:

Блинова Евгения Александровна

Минск 2020

**ЗАДАНИЕ №1:**

В основе задания – ЭК вида у2 = х3 – х + 1 (mod 751): а = –1, b = 1, р = 751, т. е. Е751(–1, 1). Задание I (рассчитано на 2 часа аудиторных занятий). 1.1 Найти точки ЭК для значений х, указанных в табл. 11.4



1.2. Разработать приложение для выполнения операций над точками кривой: а) kР, б) Р + Q, в) kР + lQ – R, г) Р – Q + R. Варианты коэффициентов приведены в табл. 11.5. В табл. 11.6 указаны координаты точек, над которыми выполняются операции.

Результаты выполнения операций представить в табличной форме.



Для начала работы нам необходимо объявить все переменные, которые приведены в таблице в соответствии с вариантом.

Для выполнения заданий необходимо написать функции, которые бы высчитывали L, x3 и y3.

Метод Lyambda() считает нам L, которое соответствует формуле: L= (y2 – y1)/(x2 – x1), если P не равно Q, но если P=Q, то L= (3(x1)^2 + a)/2y1. Продемонстрировано на рисунке 1.1.

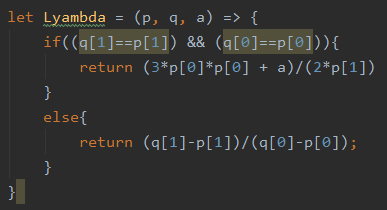


Рисунок 1.1 – Метод Lyambda()

Метод xyR() считает x3 и y3. Формула x3: x3=L^2-x1-x2, а y3: y3=L(x1-x3) - y1. Функция показана на рисунке 1.2.

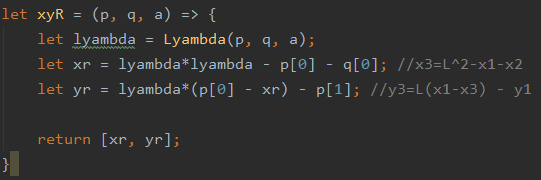


Рисунок 1.2 – Метод xyR ()

Для выполнения операций над точками кривой: а) kР, функция, которая выполняет данное действие показана на рисунке 1.3.

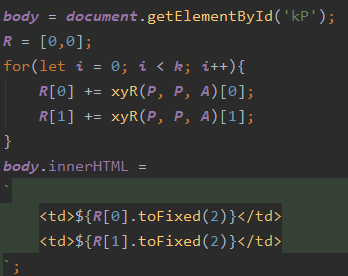


Рисунок 1.3 – Высчитываем kР

б) Р + Q, функция, которая выполняет данное действие показана на рисунке 1.4.

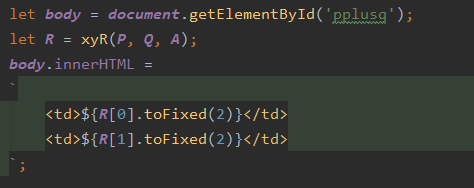


Рисунок 1.4 – Высчитываем Р + Q

в) kР + lQ – R, функция, которая выполняет данное действие показана на рисунке 1.5.

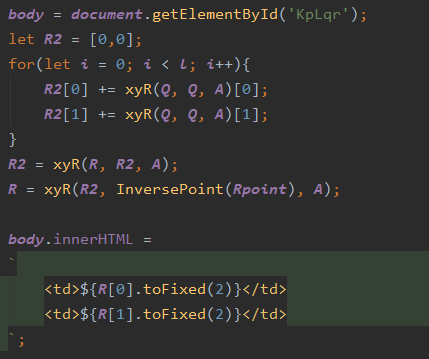


Рисунок 1.5 – Высчитываем kР + lQ – R

г) Р – Q + R. функция, которая выполняет данное действие показана на рисунке 1.6.

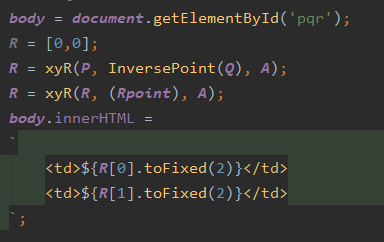


Рисунок 1.6 – Высчитываем Р – Q + R

И наконец для построения таблицы значений x, y была разработана функция ECpoints(). В которой мы высчитываем y по формуле: у2 = х^3 – х + 1 (mod 751), а х является точка из промежутка X = [481,515]. Код реализации данного задания показан на рисунке 1.7.

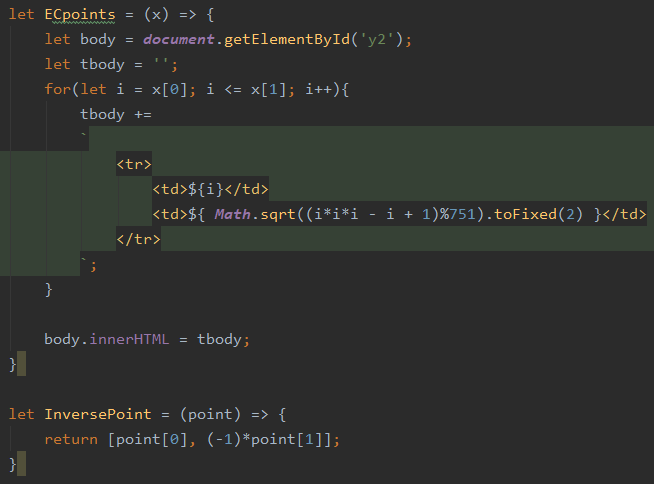


Рисунок 1.7 – Построение таблицы

Итог выполнения данного задания показан на рисунке 1.8 и 1.9.

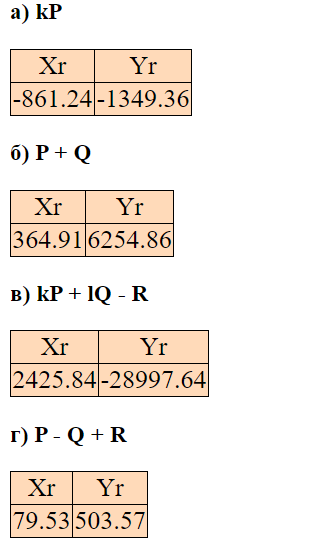


Рисунок 1.8 – Выполнения заданий пунктов а, б, в, г

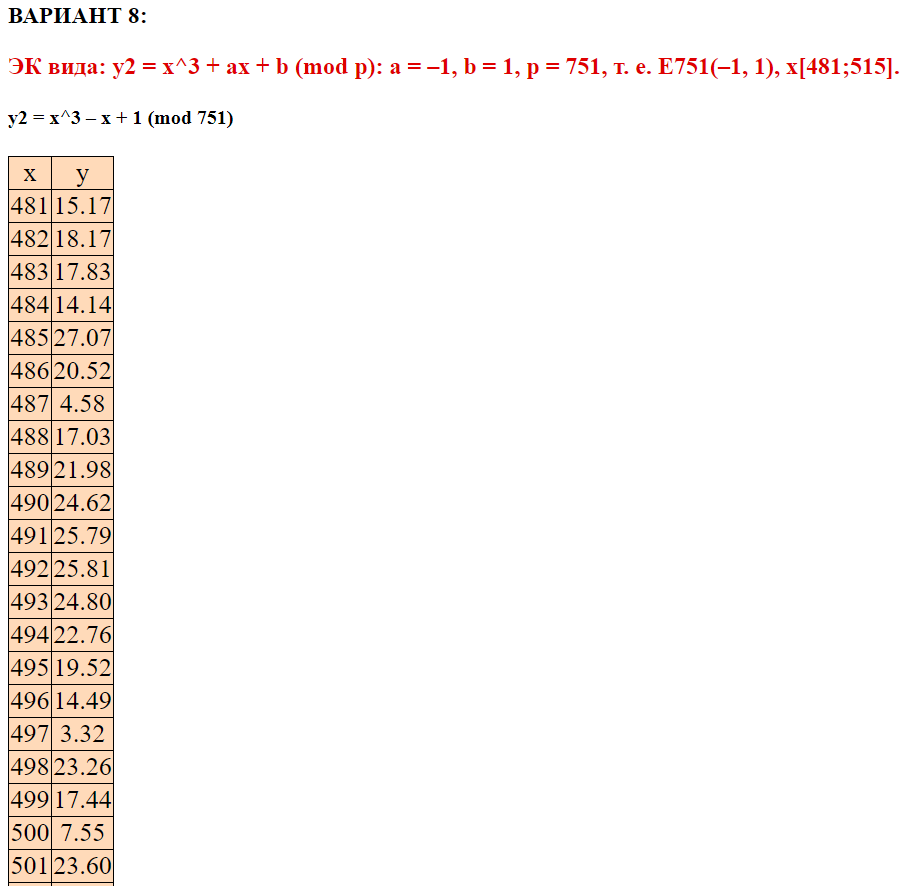


Рисунок 1.9 – Построение таблицы значений х и y

# Вывод

В данной лабораторной работе было рассмотрено понятие эллиптической кривой, особенности операций с её точками и было создано приложение, реализующее эти операции.