Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование криптографических алгоритмов на основе

эллиптических кривых.

Задание 1.

Студент: Димитриади А.В.

ФИТ 3 курс 5 группа

Преподаватель:

Савельева Маргарита Геннадьевна

Минск 2023

## 1. Описание приложения

Приложение позволяет выполнить следующие задачи:

* найти точки ЭК для значений *х*;
* выполнить операции над точками кривых;

## 2. Методика выполнения поставленных задач

Эллиптическая кривая (ЭК) определяется уравнением вида:

где *a* и *b* - параметры кривой, которые определяют ее форму и положение.

Определения:

* Бесконечно удаленная точка *O*: Это особая точка на кривой, которая представляет собой "бесконечность". Она служит нейтральным элементом для операции сложения точек.
* Аффинные координаты точки: Для представления точки (*x*, *y*) на эллиптической кривой используются аффинные координаты. *x* и *y* - это обычные координаты точки.
* Групповая операция сложения точек: На эллиптической кривой определена операция сложения точек, которая позволяет складывать две точки и получать третью точку на кривой. Операция сложения обладает свойствами ассоциативности, коммутативности и наличия нейтрального элемента.
* Удвоение точки: Удвоение точки *P* на эллиптической кривой означает сложение точки *P* с самой собой.
* Умножение точки на скаляр: Умножение точки *P* на скаляр *k* - это повторное применение операции сложения точек: *P* + *P* + *P* + ... + *P* (*k* раз).
* Порядок точки: Порядок точки *P* - это количество точек на эллиптической кривой, которые могут быть получены путем умножения точки *P* на скаляр.
* Циклическая подгруппа: Подгруппа на эллиптической кривой, которая состоит из всех точек, полученных путем умножения определенной точки на скаляры. Циклическая подгруппа имеет свой порядок, который является делителем порядка кривой.

Функции ЭК, предназначенные для выполнения данного задания, представлены на рисунке 2.1.

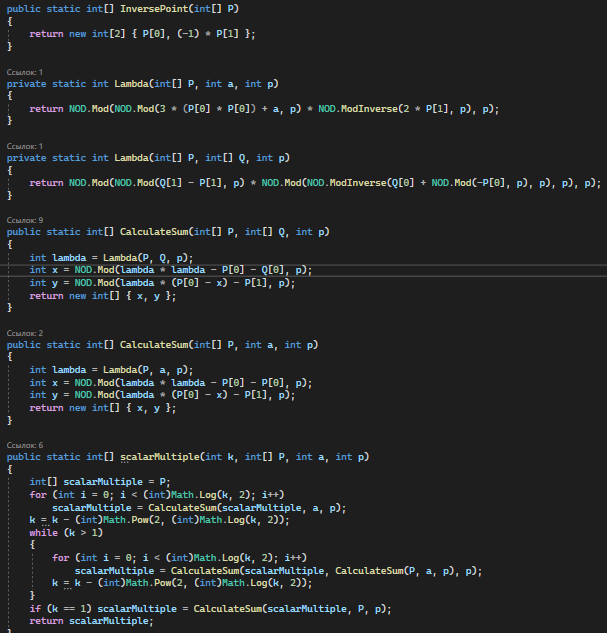


Рисунок 2.1 – Функции для работы с ЭК

В основе лежит задание ЭК вида = – *х* + 1 (mod 751): *а* = –1, *b* = 1, *р* = 751, т.е. (–1, 1), основной код и результат выполнения задания представлен на рисунке 2.2.

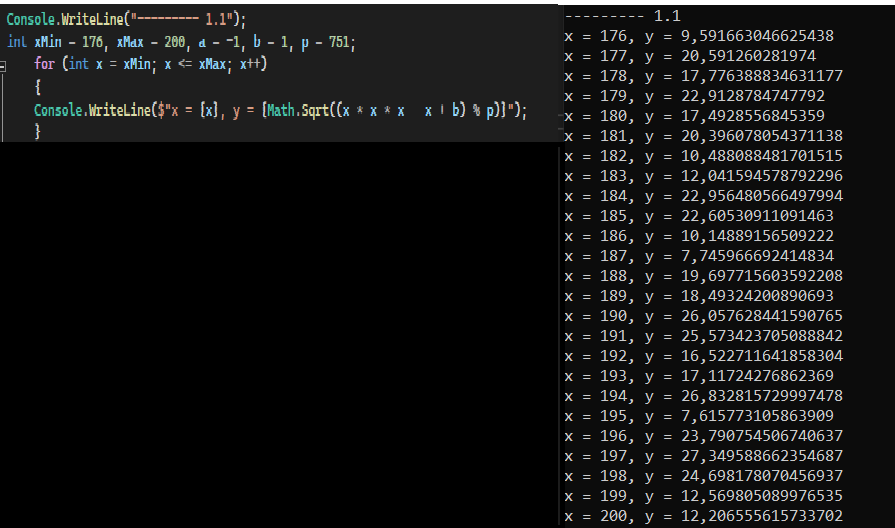


Рисунок 2.2 – Результат выполнения ЭК

Также следовало разработать приложение для выполнения операций над точками кривой: *kР*, *Р* + *Q*, *kР* + *lQ* – *R*, *Р* – *Q* + *R*.

Результат выполнения и код представлен на рисунке 2.3.

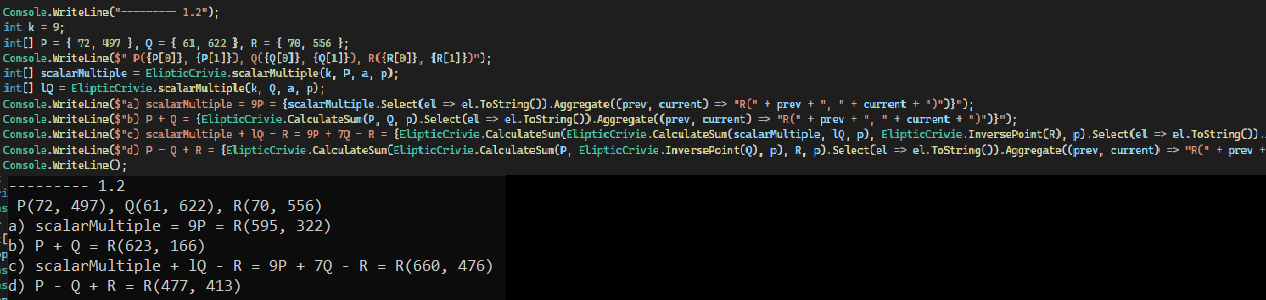


Рисунок 2.3 – Результат работы над точками кривых

## 3. Анализ результатов

Для анализа результатов было принято решение проверки корректности данных через сторонее приложение, рисунок 3.1.

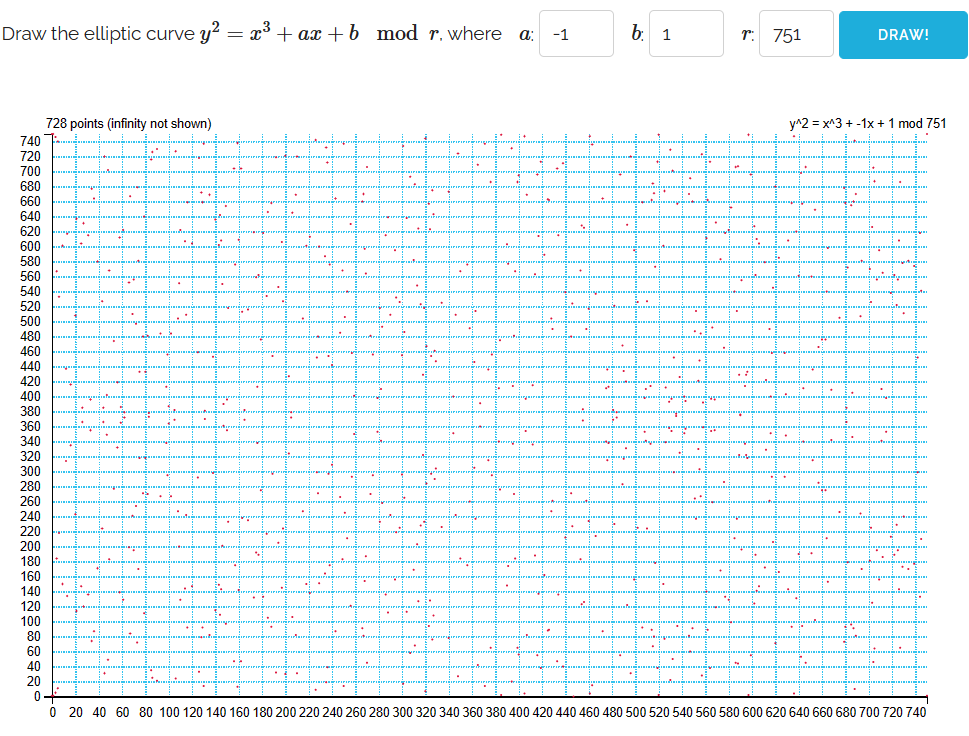


Рисунок 3.1 – Проверка корректности данных через онлайн приложение  
(источник : [Elliptic Curves over Finite Fields (graui.de)](https://graui.de/code/elliptic2/))

Проанализировав график, можно сделать вывод, что точки,которые были найдены в разработанном приложении выявлены корректно (часть точек на графике не отрисовывает ввиду того что их очень много).

## Вывод

В ходе лабораторной работы было разработано приложение для реализации сложения точек эллиптической кривой, умножения данных точек на число, нахождения обратной точки. Усвоены навыки работы с ЭК, и с их основными методами.