Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование криптографических алгоритмов на основе эллиптических кривых. Часть 1

Студент: Николаева Е.В.

ФИТ 3 курс 5 группа

Преподаватель:

Савельева Маргарита Геннадьевна

Минск 2023

1. **Описание приложения**

Приложение написано на языке программирования C# и позволяет выполнить 2 задачи:

* Найти точки ЭК для значений х;
* выполнения операций над точками кривой;

1. **Методика выполнения поставленных задач**

Эллиптические кривые – математический объект, который может быть определен над любым полем. Эллиптическая кривая над вещественными числами – это множество точек, описываемых уравнением *у*2 = *х*3 + *aх* + *b*(mod*p*), где *a* = –1, *b* = 1, *p* = 751.

Указанные точки *P* (59, 365), *Q* (59, 386), *R* (105, 382), а *k* = 7, *l* = 7.

Для реализации первой части задания применим указанную выше формулу ЭК для вычисления ординат, соответствующих абсциссам из диапазона. Выполнение данной задачи продемонстрирована на рисунках 2.1, 2.2.

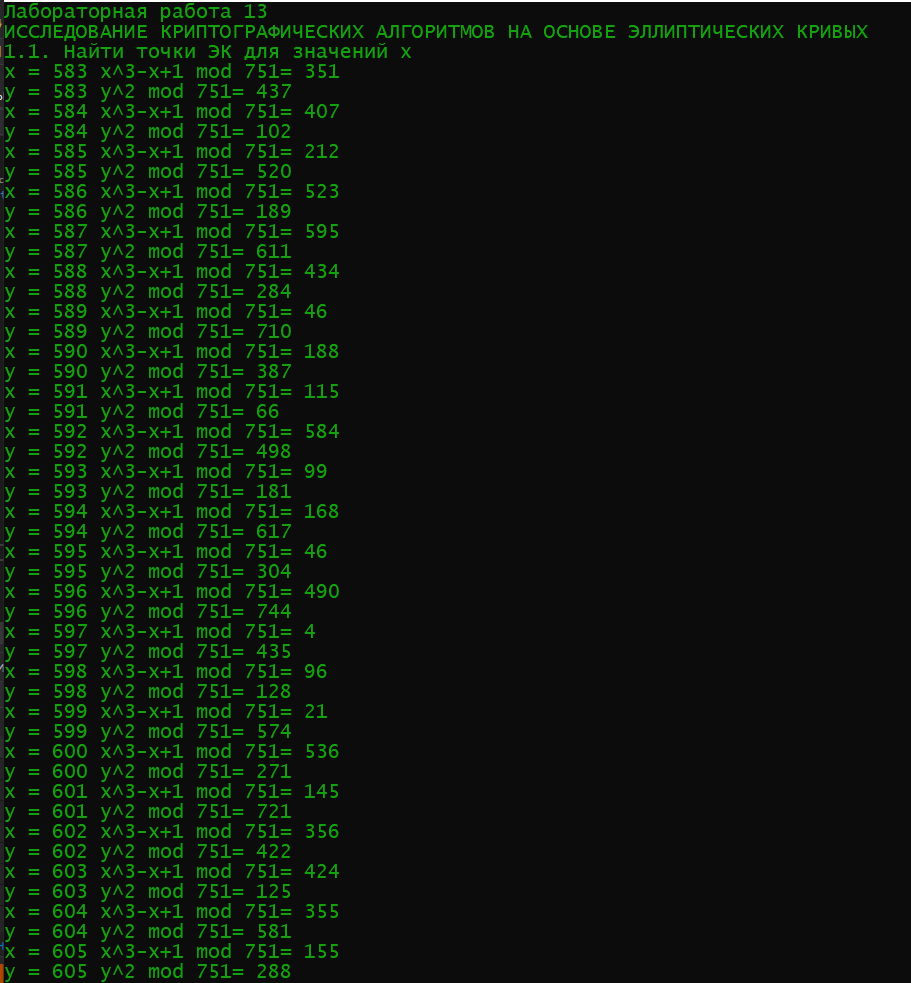


Рис. 2.1 – Выполнение функции нахождения всех точек эллиптической кривой

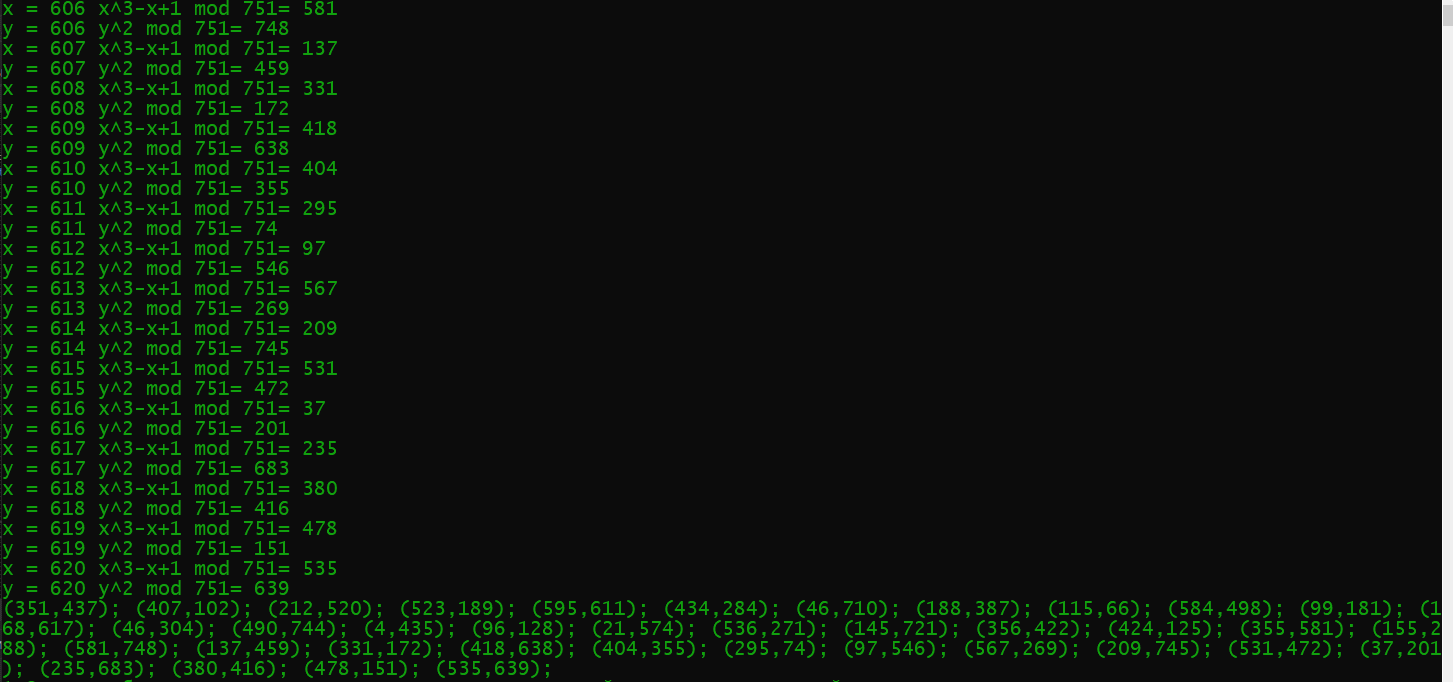


Рис. 2.2 – Выполнение функции нахождения всех точек эллиптической кривой

Во втором задании было необходимо провести операции над точками. Все созданные выражения основаны на обычных операциях, что направлены на точки. Все функции приведены на рисунках 2.3, 2.4.

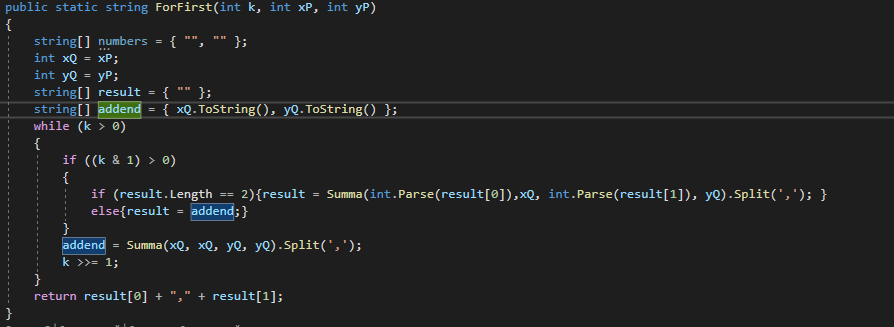


Рис. 2.3 – Функция перемножения точек

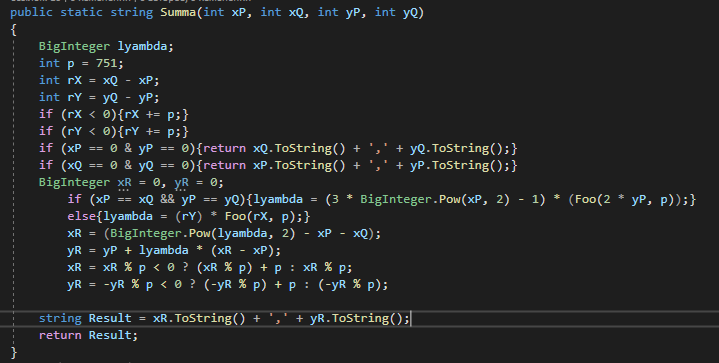


Рис. 2.4 – Функция сложения точек

Результат выполнения функция представлен на рисунке 2.5.

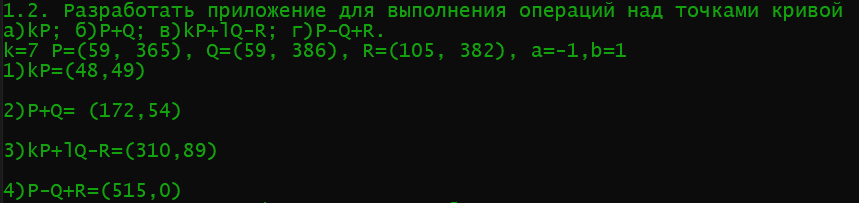


Рис. 2.5 – Результат выполнения операций над точками

Посмотрим на скорость выполнения в зависимости от размера отрывка. В данном случае Xmin=586, Xmax=620. Здесь мы видим 57ms, рисунок 2.6.

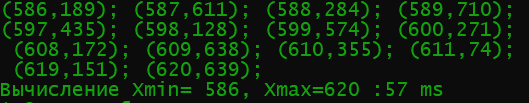


Рис. 2.6 – Выполнение функции нахождения всех точек эллиптической кривой

В данном случае Xmin=500, Xmax=620. Здесь мы видим 145ms, рисунок 2.7.

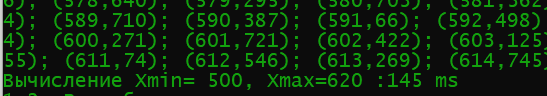


Рис. 2.7 – Выполнение функции нахождения всех точек эллиптической

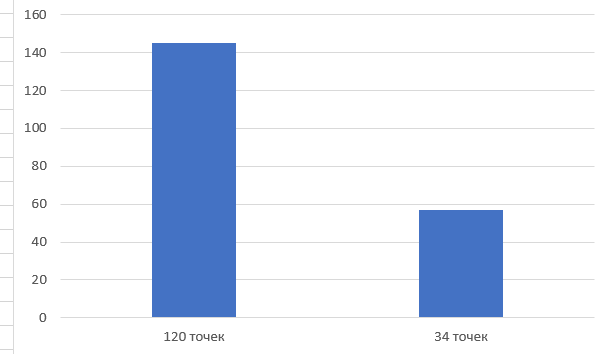


Рис. 2.8 – График зависимости скорость/количество точек

Как видно, что логично, что при увеличении точек увеличивается время вычисления, но мы можем сэкономить время, вычисляя при этом сразу один большой объем точек, чем несколько раз по маленькому массиву.

**Вывод**

В ходе лабораторной работы было разработано приложение для реализации сложения точек эллиптической кривой, умножения данных точек н число, нахождения обратной точки и комбинирования упомянутых алгебраических операций при решении задач.