Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование криптографических алгоритмов  
на основе эллиптических кривых

**Задание I**

Студент: Шулаков А.А.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М.Г.

Минск 2023

## 1. Описание приложения

Приложение написано на языке программирования C# и позволяет найти точки ЭК для значений х в диапазоне [691, 715]. Также приложение реализиует следующие операции над точками эллиптической кривой:

* *kP;*
* *P + Q;*
* *kP + lQ – R;*
* *P – Q + R.*

## 2. Методика выполнения поставленных задач

В основе задания – ЭК вида *y2 = x3 + ax + b (mod* 751): *a* = –1, *b* = 1, *p* = 751, т.е. *E*751(–1, 1).

Указанные точки *P* (70, 556), *Q* (56, 419), *R* (86, 726). За числовые коэффициенты примем *k* = 10, *l* = 3.

Для реализации первой части задания применим указанную выше формулу ЭК для вычисления ординат, соответствующих абсциссам из диапазона [691; 715]. Реализация данной задачи продемонстрирована на рисунке 2.1.

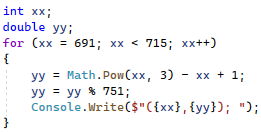


Рис. 2.1 – Вычисление ординат

Результат выше изложенных вычислений приведен на рисунке 2.2.



Рис. 2.2 – Результат вычисления точек

Далее проведем указанные в задании операции. Все выражения состоят из простейших алгебраических операций над точками эллиптической кривой: умножения на коэффициент, сложения точек, вычисление обратной точки.

Рассмотрим сложение точек. Первоначально необходимо проверить, выполняется ли для данной эллиптической кривой неравенство: *4a3*+27*b2* ≠ 0, где *a* = –1, *b* = 1.

Далее необходимо найти *λ* - угловой коэффициент секущей, проведенной через точки P, Q. Он равен:

*λ* = ( *у*2 – *у*1)/( *х*2 – *х*1), если *P≠Q*,

*λ* = (3(*х*1) 2+*а*)/2 *у*1, если *P=Q*.

Программная реализация нахождения *λ* продемонстрирована на рисунке 2.3.

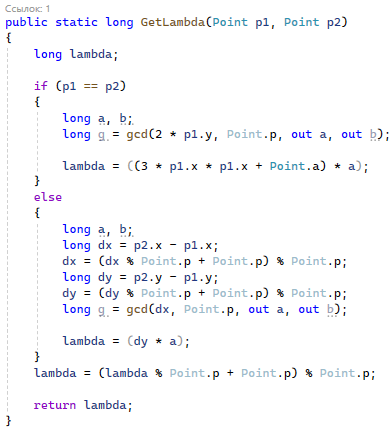


Рис. 2.3 – Нахождение *λ*

Далее предположим, что точка *P* имеет координаты (x1, *y*1), тогда *Q* (*x*2,*y*2), *R*(*x*3, *y*3) – сумма точек *P* и *Q*. Тогда координаты точки R вычисляются по формулам:

*x*3= *λ*2 – *х*1 – *х*2

*у*3= *λ*(*х*1–*х*3 ) – *у*1

Программная реализация сложения двух точек ЭК продемонстрирована на рисунке 2.4.

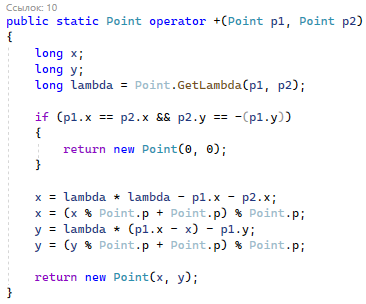


Рис. 2.4 – Сложение точек ЭК

Далее рассмотрим алгоритм нахождения произведения точки и числа. По правилу умножения точки ЭК, для умножения *Pz* необходимо точку *Р* сложить саму с собой *z* раз. Программная реализация данной операции приведена на рисунке 2.5.

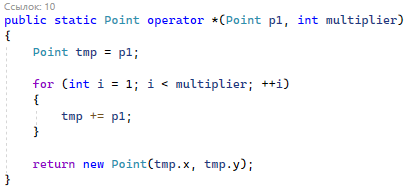


Рис. 2.5 – Умножение точки на число

Также в указанных вычислениях необходимо было применять сложение с инверсией: инверсией по отношению к точке (*x*,*y*) является точка (*x*,-*y*) на ЭК.

Результаты вычислений указанных в задании выражений по выше упомянутым формулам, представлен на рисунке 2.6.

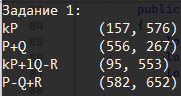


Рис. 2.6 – Результаты вычислений

# **3.Анализ результатов**

Анализ результатов операций будет зависеть от конкретных точек и параметров, используемых в операциях. Результаты могут варьироваться в зависимости от выбранных точек, значения скаляров и применяемых операций.

Важно учитывать, что операции на эллиптических кривых выполняются над элементами поля, которое в данном случае является полем по модулю 751. Поэтому все вычисления производятся в этом поле с использованием арифметики по модулю 751.

Результаты операций могут представлять собой точки на эллиптической кривой или бесконечно удаленную точку (нейтральный элемент группы точек на кривой). Результаты также могут зависеть от правил сложения и умножения точек на эллиптической кривой, которые определяются соответствующими алгоритмами.

При разработке приложения для выполнения этих операций, важно убедиться в правильной реализации алгоритмов сложения, умножения и вычитания точек на эллиптической кривой, а также в правильном использовании арифметики по модулю 751. Также следует учесть возможные исключительные ситуации, такие как деление на ноль или обработку бесконечно удаленной точки.

Итоговый анализ результатов будет зависеть от конкретной реализации и использования операций над точками кривой в данном приложении.

## 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.