Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование криптографических алгоритмов  
на основе эллиптических кривых

**Задание I**

Студент: Чистякова Ю.А.

ФИТ 3 курс 5 группа

Преподаватель: Берников В.О.

Минск 2020

## 1. Описание приложения

Приложение написано на языке программирования C# и позволяет найти точки ЭК для значений х в диапазоне [716, 750]. 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. E751(–1, 1).

Указанные точки P (67, 84), Q (69, 241), R (66, 199). За числовые коэффициенты примем k = 11, l - 5.

Для реализации первой части задания применим указанную выше формулу ЭК для вычисления ординат, соответствующих абсциссам из диапазона [716; 750]. Реализация данной задачи продемонстрирована на рисунке 2.1.

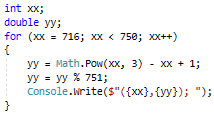


Рис. 2.1 – Вычисление ординат

Результат выше изложенных вычислений приведен на рисунке 2.2.

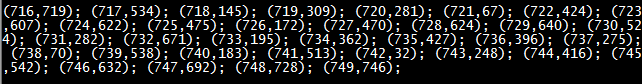


Рис. 2.2 – Результат вычисления точек

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+27b2 ≠ 0, где a = –1, b = 1.

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

λ = ( у2 – у1)/( х2 – х1), если P≠Q,

λ = (3(х1) 2+а)/2 у1, если P=Q.

Программная реализация нахождения λ продемонстрирована на рисунке 2.3.

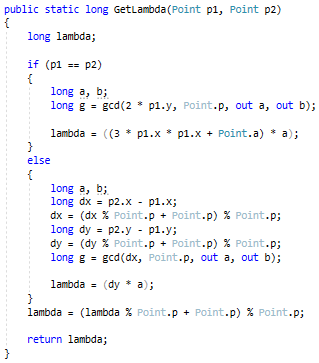


Рис. 2.3 – Нахождение λ

Далее предположим, что точка P имеет координаты (x1, y1), тогда Q (x2,y2), R(x3, y3) – сумма точек P и Q. Тогда координаты точки R вычисляются по формулам:

x3= λ 2 – х1 – х2

у3= λ (х1–х3 ) – у1

Программная реализация сложения двух точек ЭК продемонстрирована на рисунке 2.4.

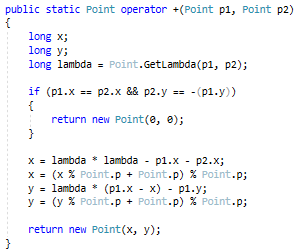


Рис. 2.4 – Сложение точек ЭК

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.

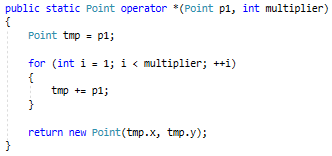


Рис. 2.5 – Умножение точки на число

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.

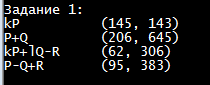


Рис. 2.6 – Результаты вычислений

## 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.