ЛАБОРАТОРНАЯ РАБОТА №1

НАХОЖДЕНИЕ ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

ЦЕЛЬ РАБОТЫ: приобретение практических навыков в построении эллиптических кривых.

**Введение**

Одной из важных задач в алгебраической геометрии является задача нахождения элементов группы точек эллиптической кривой.

**Теория**

Уравнение элептической кривой над произвольным полем может быть сведено к обобщенной форме Вейерштрасса:

.

Корни выше указанного уравнения группу, причем указанная группа циклическая. Поскольку группа является циклической, то ее можно построить используя образующий элемент.

Введем операцию сложения двух точек эллиптической кривой.

Сложение точек P1 + P2 = P3 , где , задается следующими формулами:

1. Если , то .(0,0)
2. ;
3. Если , то:

,

,

где



1. Если :

,

**Частный вид элептической кривой над полем простых чисел:**

Если кривая задана уравнением , где , то можно записать следующее:

Сложение переписывается как :

1. Если :

,

,

.

1. Если :

,

,

.

**Рабочее задание**

Пусть даны следующие условия:

GF(31991), 

Количество точек на этой кривой n=32089

В качестве генератора можно взять точку: G=(0,5585)

Точка бесконечности 0=(0,0).

**Задание:** Написать программу, генерирующую точки эллиптической кривой.

**Требования к реализации:**

1. Сгенерированные точки должны выводится на экран графически.
2. Количество точек сгенерированных точек должно выводится на экран.
3. Все опереции с элептическими кривыми должны быть написанны засотоятельно, а не взяты со сторонних библеотек.