1. Министерство науки и высшего образования Российской Федерации
2. Санкт-Петербургский политехнический университет Петра Великого
3. Институт компьютерных наук и кибербезопасности
4. Высшая школа кибербезопасности

**ЛАБОРАТОРНАЯ РАБОТА № 5**

1. «Арифметика эллиптических кривых»
2. по дисциплине «Быстрые вычислительные алгоритмы»
3. Выполнил
4. студент гр. 5151001/00201 Устюгов А.А.

<*подпись*>

1. Преподаватель д.т.н. Шенец Н.Н.

<*подпись*>

1. Санкт-Петербург
2. 2024

# Цель работы

Изучение и освоение алгоритмов арифметики группы точек эллиптической кривой.

# Задание

Написать программу, которая реализует арифметические операции в группе точек эллиптической кривой в соответствии с вариантом задания. Программа должна позволять задавать параметры эллиптической кривой, задавать точку аффинными координатами и проверять ее принадлежность кривой, генерировать случайную точку эллиптической кривой, выполнять сложение двух произвольных указанных точек.

# Ход работы

Программа написана на C++ с использованием библиотеки NTL. Вариант 6: удвоение в координатах Чудновского, сложение в смешанных чудновско-аффинных координатах.

Был написан класс эллиптической кривой в краткой форме Вейерштрасса, а также класс точки. Класс кривой принимает характеристику поля и коэффициенты A, B. Точку можно задать как аффинными координатами, так и сразу в координатах Чудновского. Также можно задать как бесконечно удаленную.

Сложение в координатах Чудновского выглядит следующим образом:

Удвоение следующим:

Было решено писать сложение не в смешанных координатах, а в координатах Чудновского, так как каждый раз приводить точку к аффинной будет дороже, чем 2 лишние операции умножения.

Для проверки принадлежности аффинной точки к кривой необходимо отдельно посчитать правую и левую части кривой и прировнять их. Если совпадает, то точка принадлежит кривой, иначе нет.

Для генерации случайной точки я случайно выбираю *x*-координату, вычисляю правую часть уравнения эллиптической кривой и беру символ Якоби по модулю характеристики поля. Если в результате получится 0 или 1, то вычисляю корень в поле и получаю *y*-координату, иначе продолжаю случайно выбирать *x*-координату.

Далее сгенерируем случайную точку P и проверим, что она принадлежит группе точек кривой. Также удвоим и утроим полученную точку.

На рисунке 1 представлены сгенерированная точка, bool значение о принадлежности кривой и координаты удвоенной и утроенной точки. На рисунке 2 представлено удвоение и утроение точки в SageMath для проверки полученных вычислений.

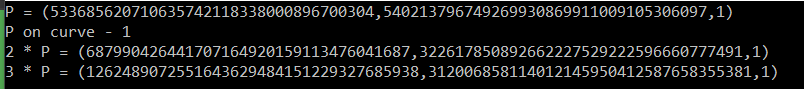


Рисунок 1 – результаты моей программы

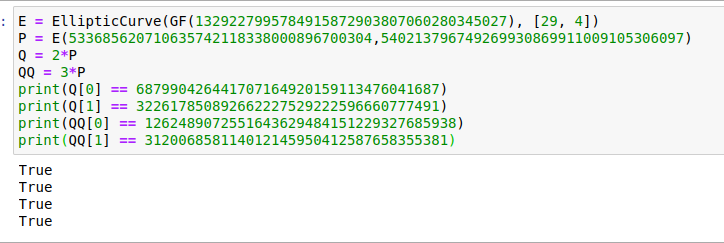


Рисунок 2 – проверка результата в SageMath

На рисунке 4 представлен результат работы на тесте из методического пособия, на 5 проверка в Sage.

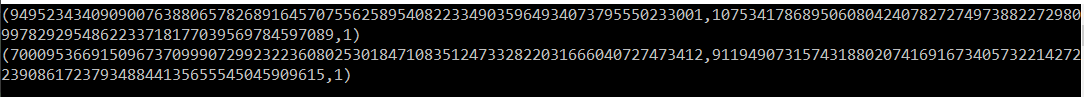


Рисунок 4 – результат моей программы на тесте из методического пособия

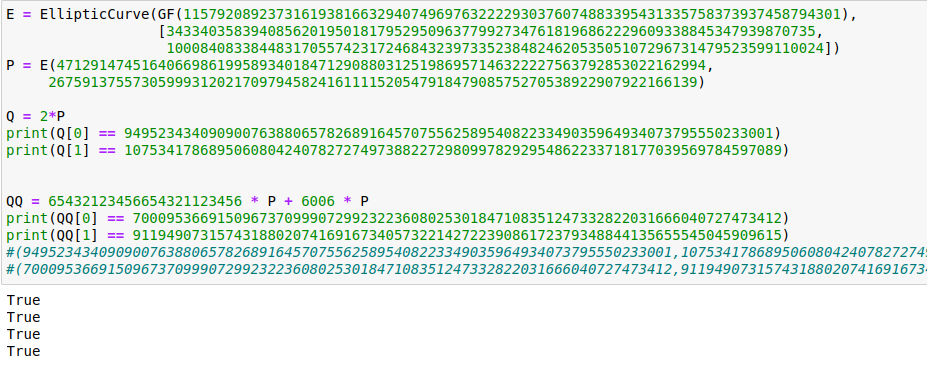


Рисунок 5 – проверка в Sage

# Контрольные вопросы

1. Какие кривые называют особыми?

Особой называют кривую, которая содержит точку, у которой все частные производные равны нулю.

1. Что такое «допустимая замена переменных»? Как это понятие связанно с группами рациональных точек соответствующих кривых?

Допустимая замена переменных – замена, сохраняющая j-инвариант кривой. Две кривые называются изоморфными, если переход между ними возможен с помощью допустимой замены переменных.

1. При каких условиях существуют формы Гессе, Монтгомери и Эдвардса эллиптической кривой?

Форма Монтгомери существует в поле, характеристика которого отлична от 2. Коэффициенты *B* и *С* таковы, что .

Форма Эдвардса существует в поле, характеристика которого отлична от 2. Коэффициенты c и d таковы, что . Вообще существует бинарная форма Эдвардса, но ее вид значительно отличается.

Форма Гессе существует в поле любой характеристики. Коэффициент .

# Вывод

В результате данной работы были изучены различные системы координат для сложения точек эллиптической кривой. Был реализован класс точки и класс эллиптической кривой, переопределены операции сложения, умножения точки на число, генерации случайной точки. В целом, если дописать алгоритм Чуфа или алгоритм SEA для подсчета числа точек кривой, то данный класс можно использовать как минимальный набор для работы с эллиптическими кривыми.