БФУ им. И. Канта – Компьютерный практикум по криптографии на эллиптических кривых

Преподаватель С. Новоселов 2021

Лабораторная работа № 3

Опубликована **30.09.2021**

Дедлайн **21.10.2021**

Разработать программу в системе компьютерной алгебры Sage, реализующую следующие функции:

1. `nTorsion_extension_deg(n, a, b, q)`, где `a, b` – коэффициенты эллиптической кривой $E : y^2 = x^3 + ax + b$, заданной над полем $\mathbb{F}_q$, где q - простое, $\neq 2, 3$, $n \geq 3$. Функция возвращает $d = [K_{E,n} : K]$ – степень расширения поля $K_{E,n} = (x_1, y_1, \dots x_m, y_m)$ над $K = \mathbb{F}_q$, где $E[n] = \{\mathcal{O}, (x_1, y_1), \dots, (x_m, y_m)\}$ – точки n-кручения эллиптической кривой E.

2. `nTorsionPoints(n, a, b, q)`, те же выходные данные, что и для функции `nTorsion_extension_deg(n, a, b, q)`, но здесь $n \geq 1$. Функция возвращает все точки n-кручения кривой E.

Замечание: оптимизировать работу функций так, чтобы они терминировали за разумное время для малых и средних значений n, q.

Требования к сдаче

- Исходный код должен содержать комментарии к каждой из функций с описанием входных и выходных параметров
- Лабораторную следует выполнять модификацией файла с тестами, заменяя строку `"# your code here."`на код, реализующий функцию.
- Функции должны работать на всех примерах, что проверяется запуском команды:
  `sage -t file_with_tests.sage`
- Студент должен понимать, что он написал, зачем, а также ответить на теоретические вопросы.