

---

## Лабораторная работа № 4

Опубликована 09.10.2020

Дэдлайн 30.10.2019

---

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

1. `order_BSGS(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,  $\neq 2, 3$ . Функция реализует алгоритм Baby Step – Giant Step подсчета  $\mathbb{F}_q$ -рациональных точек кривой, и возвращает  $\#E(\mathbb{F}_q)$ .

### Требования к сдаче

- Лабораторную следует выполнять модификацией файла с тестами (`TP4_tests.sage`), заменяя строку “`# your code here.`” на код, реализующий функцию.
- Функции должны работать на всех примерах, что проверяется запуском команды:  
`sage -t TP4_tests.sage`
- Исходный код должен содержать комментарии к каждой из функций с описанием входных и выходных параметров