
Лабораторная работа № 4

Опубликована **29.09.2026**

Дэдлайн **13.10.2026**

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

1. `ec_order(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 подсчета $\mathbb{F}_q$ – рациональных точек кривой с помощью алгоритма Baby Step – Giant Step или ρ -метода Полларда, и возвращает $\#E(\mathbb{F}_q)$.

Требования к сдаче

- Функция должна быть оптимизирована так, чтобы выполняться на тестах за разумное время (около 5 минут).
- 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.