

---

## Лабораторная работа № 5

Опубликована 18.11.2020

Дэдлайн 02.12.2020

---

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

1. `factorECM(N)`, где  $N = pq$ ,  $p, q$  – простые. Функция реализует алгоритм факторизации на эллиптической кривой и возвращает либо  $(p, q)$ , либо, в случае длительных вычислений, “делители не найдены”.

Для тестирования можно пользоваться встроенной функцией, см. <http://doc.sagemath.org/html/en/reference/interfaces/sage/interfaces/ecm.html>.

### 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.