Преподаватель Е. Киршанова 2019–2020

Лабораторная работа № 5

Опубликована **01.11.2019**

Дэдлайн **22.11.2019**

Разработать программу в системе компьютерной алгебры Maple или Sage (в одной на выбор), 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

- Для программ разработанных в системе Maple, следует сдавать подгружаемый модуль.
- Исходный код должен содержать комментарии к каждой из функций с описанием входных и выходных параметров