

## Лабораторная работа №1

Преподаватель: Новосёлов Семён

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

1. `jInvariant( $a_1, a_2, a_3, a_4, a_6$ )`, где  $a_1, a_2, a_3, a_4, a_6$  – коэффициенты кривой, заданной уравнением Вейерштрасса. Если кривая является эллиптической, функция возвращает  $j$ -инвариант кривой, иначе сообщение о том, что кривая сингулярна.
2. `randIsomorphic( $a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_6 = 0$ )`, где  $a_1, a_2, a_3, a_4, a_6, a, b$  – коэффициенты эллиптической кривой  $E_1$  в общем случае, или в случае  $\text{char}(K) \neq 2, 3$ . Функция возвращает коэффициенты кривой  $E_2$ , изоморфной  $E_1$  над  $\mathbb{Q}$  путём случайного выбора параметров  $(u, r, s, t)$ . Если коэффициенты  $a_1, a_2, a_3, a_4, a_6$  задают сингулярную кривую, функция завершает с соответствующим сообщением.
3. `isIsomorphic( $a_1, a_2, a_3, a_4, a_6, \_a_1, \_a_2, \_a_3, \_a_4, \_a_6, p$ )`, где  $a_1, a_2, a_3, a_4, a_6$  – коэффициенты эллиптической кривой  $E_1$ ,  $\_a_1, \_a_2, \_a_3, \_a_4, \_a_6$  – коэффициенты эллиптической кривой  $E_2$ ,  $p$  – простое число (означает кривые заданы над  $\mathbb{F}_p$ ) или 0 (кривые заданы над  $\mathbb{Q}$ ). Функция определяет, являются ли кривые изоморфными над  $\mathbb{F}_p$  (или  $\mathbb{Q}$ ), и возвращает одно из значений  $\in \{isomorphic, non - isomorphic\}$ . Если коэффициенты  $a_1, a_2, a_3, a_4, a_6$  или  $\_a_1, \_a_2, \_a_3, \_a_4, \_a_6$  задают сингулярную кривую, функция завершает с соответствующим сообщением.
4. `findExtension( $a_1, a_2, a_3, a_4, a_6, \_a_1, \_a_2, \_a_3, \_a_4, \_a_6, p$ )`, коэффициенты эллиптической кривой  $E_1, \_a_1, \_a_2, \_a_3, \_a_4, \_a_6$  – коэффициенты эллиптической кривой  $E_2$ , заданные над  $\mathbb{F}_p$  ( $p$  интерпретировать аналогично предыдущей функции). Функция определяет, над каким полем кривые  $E_1 \simeq E_2$  и возвращает степень расширения этого поля над  $\mathbb{F}_p$ . Если коэффициенты  $a_1, a_2, a_3, a_4, a_6$  или  $\_a_1, \_a_2, \_a_3, \_a_4, \_a_6$  задают сингулярную кривую, функция завершает с соответствующим сообщением.

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.