БФУ им. И. Канта – Компьютерный практикум по криптографии на эллиптических кривых

Преподаватель Е. Киршанова 2019–2020

Лабораторная работа № 1

Опубликована **06.09.2019**

Дэдлайн **27.09.2019**

Разработать программу в системе компьютерной алгебры Maple или Sage (в одной на выбор), реализующую следующие функции:

1. `jInvariant(`$\mathtt{a}_1, \mathtt{a}_2, \mathtt{a}_3, \mathtt{a}_4, \mathtt{a}_6$`)`, где $\mathtt{a}_1, \mathtt{a}_2, \mathtt{a}_3, \mathtt{a}_4, \mathtt{a}_6$ – коэффициенты кривой, заданной уравнение Вейерштрасса. Если кривая является эллиптической, функция возвращает j-инвариант кривой, иначе сообщение о том, что кривая сингулярна.

2. `randIsomorphic(`$\mathtt{a}_1 = 0, \mathtt{a}_2 = 0, \mathtt{a}_3 = 0, \mathtt{a}_4 = 0, \mathtt{a}_6 = 0, \mathtt{a} = 0, \mathtt{b} = 0$`)`, где $\mathtt{a}_1, \mathtt{a}_2, \mathtt{a}_3, \mathtt{a}_4, \mathtt{a}_6, \mathtt{a}, \mathtt{b}$ – коэффициенты эллиптической кривой E_1 в общем случае, или в случае $\mathsf{char}(K) \neq 2, 3$. Функция возвращает коэффициенты кривой E_2, изоморфной E_1 над $\mathbb{Q}$ путём случайного выбора параметров (u, r, s, t). Если коэффициенты $\mathtt{a}_1, \mathtt{a}_2, \mathtt{a}_3, \mathtt{a}_4, \mathtt{a}_6$ задают сингулярную кривую, функция терминирует с соответствующим сообщением.

3. `isIsomorphic(`$\mathtt{a}_1, \mathtt{a}_2, \mathtt{a}_3, \mathtt{a}_4, \mathtt{a}_6, \mathtt{\_a}_1, \mathtt{\_a}_2, \mathtt{\_a}_3, \mathtt{\_a}_4, \mathtt{\_a}_6, p$`)`, где $\mathtt{a}_1, \mathtt{a}_2, \mathtt{a}_3, \mathtt{a}_4, \mathtt{a}_6$ – коэффициенты эллиптической кривой E_1, $\mathtt{\_a}_1, \mathtt{\_a}_2, \mathtt{\_a}_3, \mathtt{\_a}_4, \mathtt{\_a}_6$ – 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 $\in \{\mathtt{isomorphic}, \mathtt{non-isomorphic}\}$. Если коэффициенты $\mathtt{a}_1, \mathtt{a}_2, \mathtt{a}_3, \mathtt{a}_4, \mathtt{a}_6$ или $\mathtt{\_a}_1, \mathtt{\_a}_2, \mathtt{\_a}_3, \mathtt{\_a}_4, \mathtt{\_a}_6$ задают сингулярную кривую, функция терминирует с соответствующим сообщением.

4. `findExtension(`$\mathtt{a}_1, \mathtt{a}_2, \mathtt{a}_3, \mathtt{a}_4, \mathtt{a}_6, \mathtt{\_a}_1, \mathtt{\_a}_2, \mathtt{\_a}_3, \mathtt{\_a}_4, \mathtt{\_a}_6, p$`)`, коэффициенты эллиптической кривой E_1, $\mathtt{\_a}_1, \mathtt{\_a}_2, \mathtt{\_a}_3, \mathtt{\_a}_4, \mathtt{\_a}_6$ – коэффициенты эллиптической кривой E_2, заданные над $\mathbb{F}_p$ (p интерпретировать аналогично предыдущей функции).Функция определяет, над каким полем кривые $E_1 \cong E_2$ и возвращает степень расширения этого поля над $\mathbb{F}_p$.

   Если коэффициенты $\mathtt{a}_1, \mathtt{a}_2, \mathtt{a}_3, \mathtt{a}_4, \mathtt{a}_6$ или $\mathtt{\_a}_1, \mathtt{\_a}_2, \mathtt{\_a}_3, \mathtt{\_a}_4, \mathtt{\_a}_6$ задают сингулярную кривую, функция терминирует с соответствующим сообщением.

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