

---

## Лабораторная работа № 2

Опубликована 21.09.2023

Дедлайн 05.10.2023

---

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

1. `Sum(a, b, q, x1, y1, x2, y2)`, где  $a, b$  – коэффициенты эллиптической кривой  $E$ , заданной над полем  $\mathbb{F}_q$ ,  $q$  – простое,  $\neq 2, 3$ ,  $P_1 = (x1, y1), P_2 = (x2, y2)$  – точки на  $E$  ( $y_i = \text{infinity}$  для  $P_i = \mathcal{O}$ ). Функция возвращает координаты  $P_3 = (x3, y3) = P_1 + P_2$ . Если  $P_1$  или  $P_2$  не лежат на  $E$ , функция возвращает ошибку.
2. `SumProj(a, b, q, x1, y1, z1, x2, y2, z2)`, те же параметры и выходные данные, что и для функции `Sum(a, b, q, x1, y1, x2, y2)`, но точки  $P_1, P_2$  заданы в проективных координатах. Вычисления проводятся также с проективными координатами.
3. `Mul(a, b, q, x1, y1, k)`, где  $a, b$  – коэффициенты эллиптической кривой  $E$ , заданной над полем  $\mathbb{F}_q$ , где  $q$  – простое,  $\neq 2, 3$ ,  $P_1 = (x1, y1) \in E$ ,  $k \in \mathbb{Z}$ . Функция возвращает координаты точки  $P_k = (x_k, y_k) = k \cdot P_1$ . Если  $P_1 \notin E$ , функция возвращает ошибку.

### 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.