

Семинар 13. Эллиптические кривые.

Введение в теорию чисел, весенний семестр 2023 г.

ФАКУЛЬТЕТ МАТЕМАТИКИ, НИУ ВШЭ

Во всех задачах этого листка в качестве нулевого элемента в группе точек на эллиптической кривой выбирается бесконечно удалённая точка.

Задача 1. Эллиптическая кривая E над \mathbb{Q} задана уравнением

$$y^2 = x^3 - 2.$$

- (а) Найдите дискриминант и j -инвариант кривой E .
- (б) Для каких простых чисел p кривая $E(\mathbb{F}_p)$ имеет особенность? Какого типа эта особенность?
- (в) Найдите количество точек на $E(\mathbb{F}_p)$ для $p = 5$ и $p = 7$.
- (г) Найдите группу кручения $E_{tors}(\mathbb{Q})$ в группе всех рациональных точек $E(\mathbb{Q})$.

Задача 2. Эллиптическая кривая над \mathbb{Q} задана уравнением

$$y^2 + y = x^3 - x^2.$$

Через P обозначим точку $(0, 0)$ на кривой.

- (а) Найдите координаты точки $2P$.
- (б) Найдите координаты суммы точек $P + Q$, где $Q = (1, -1)$.
- (в) Найдите координаты точки $2Q$.
- (г) Найдите порядок циклической подгруппы, порождённой точкой P .

Задача 3. Эллиптическая кривая задана над \mathbb{Q} уравнением

$$y^2 = x^3 + 1.$$

Через P обозначим точку $(2, 3)$ на кривой.

- (а) Найдите координаты точки $2P$.
- (б) Найдите координаты суммы точек $P + Q$, где $Q = (0, 1)$.
- (в) Пусть $R = (-1, 0)$. Найдите координаты точки $2R$.
- (г) Найдите порядок циклической подгруппы, порождённой точкой P .

Задача 4. Эллиптическая кривая над \mathbb{Q} задана уравнением

$$y^2 + xy + y = x^3 - x^2 - 3x + 3.$$

Через P обозначим точку $(1, 0)$ на кривой.

- (а) Найдите координаты точки $2P$.
- (б) Найдите координаты суммы точек $P + Q$, где $Q = (-1, -2)$.
- (в) Пусть $R = (3, -6)$. Найдите координаты точки $2R$.
- (г) Найдите порядок циклической подгруппы, порождённой точкой P .

Задача 5. Для каждой эллиптической кривой E из задач 2–4 найдите группу кручения $E_{tors}(\mathbb{Q})$.