Плоские кривые. Геометрия эллиптических кривых.

Задача 1. a) Пусть C_f и C_g — плоские кривые степеней m и n соответственно. Предположим, что кривые пересекаются в точках $P_1, \ldots, P_t$, при этом порядок P_i на C_f равен r_i, а порядок P_i на C_g равен s_i. Убедитесь, что $\sum\limits_{i=1}^{t} r_i s_i \leq mn$.

b) Пусть C_f — кривая степени m без кратных компонент с особыми точками P_i порядка r_i. Покажите, что $\sum r_i(r_i - 1) \leq m(m-1)$.

Подсказка: посмотрите на подходящую производную f.

c) Пусть C_f — *неприводимая* кривая степени m с особыми точками P_i порядка r_i. Покажите, что $\sum r_i(r_i - 1) \leq (m-1)(m-2)$.

Подсказка: рассмотрите подходящую производную f, имеющую порядок $r_i - 1$ в P_i, а также $\left[\frac{(m-1)(m+1)}{2}\right]$-мерное семейство всех кривых степени $m-1$ и подсемейство кривых, имеющих порядок $r_i - 1$ в P_i.

d) Рассмотрев семейство прямых, проходящих через одну точку и кривую $x^n + wy^{n-1} = 0$, убедитесь, что неравенства из предыдущих пунктов точные.

Задача 2°. Покажите, что в характеристике 0 квадрика C_F неприводима тогда и только тогда, когда 3×3 матрица ее частных производных имеет ненулевой определитель. Когда это утверждение остается верным в характеристике p?

Задача 3. a) Докажите, что над полем характеристики ноль точка P на проективной кривой C_F, заданной уравнением $F(x_1, x_2, x_3) = 0$, является точкой перегиба тогда и только тогда, когда линейная форма, составленная из первых производных, делит квадратичную форму с коэффициентами из вторых производных.

b) Покажите, что в характеристике ноль точка P на кривой C_F является точкой перегиба тогда и только тогда, когда гессиан $H(x_1, x_2, x_3) = \det\left(\frac{\partial^2 F}{\partial x_i \partial x_j}\right)$ в этой точке обращается в ноль.

c) Когда предыдущие утверждения верны в характеристике p?

d) Покажите, что неособая проективная кривая степени ≥ 3 над алгебраически замкнутым полем имеет по крайней мере одну точку перегиба.

Задача 4°. Найдите особые точки и касательные в них для следующих кривых в $\mathbb{A}^2$:
a) $y^2 = x^3$; b) $4x^2y^2 = (x^2 + y^2)^3$; c) $y^2 = x^4 + y^4$.

Задача 5°. При каких a и b следующие проективные кривые особы:
a) $y^2z + axyz + byz^2 = x^3$; b) $y^2z = x^3 + axz^2 + bz^3$.

Задача 6°. a) Пусть C — кривая $y^2z = x^3$. Покажите, что отображение $\phi\colon \mathbb{P}^1 \to C$, заданное как $\phi([s,t]) = [s^2t, s^3, t^3]$, является регулярным морфизмом. Найдите обратное рациональное отображение $\psi\colon C \to \mathbb{P}^1$. Является ли ψ изоморфизмом?

b) Ответьте на налогичные вопросы для $C\colon y^2z = x^3 + x^2z$ и отображения $\phi([s,t]) = [(s^2 - t^2)t, (s^2 - t^2)s, t^3]$.

Задача 7° (морфизм Фробениуса). Пусть $C \subset \mathbb{P}^2$ — кривая над конечным полем $\mathbb{F}_q$.
a) Покажите, что $\phi\colon [x, y, z] \mapsto [x^q, y^q, z^q]$ определяет биективный морфизм из C в C.
b) Является ли этот морфизм изоморфизмом?
c) Убедитесь, что $C(\mathbb{F}_q) = \{P \in C \mid \phi(P) = P\}$.

Задача 8°. Пусть C_p — кривая в $\mathbb{P}^2$, заданная уравнением $x^2 + y^2 = pz^2$.
a) Докажите, что C_p изоморфна $\mathbb{P}^1$ над $\mathbb{Q}$ тогда и только тогда, когда $p \equiv 1 \mod 4$.
b) Покажите, что при $p \equiv 3 \mod 4$ эти кривые попарно не изоморфны над $\mathbb{Q}$ и не изоморфны $\mathbb{P}^1$.

Задача 9 (кривые и группа Галуа).

a) Пусть C_f/k — аффинная кривая. Покажите, что $k[C_f] = k[x,y]/(f(x,y)) = \{f \in \bar{k}[C] \mid \sigma(f) = f$ для всех $\sigma \in \mathrm{Gal}(\bar{k}/k)\}$.

b) Докажите, что $\mathbb{P}^2(k) = \{P \in \mathbb{P}^2(\bar{k}) \mid \sigma(P) = P$ для всех $\sigma \in \mathrm{Gal}(\bar{k}/k)\}$.

c) Пусть $\phi\colon C_1 \to C_2$ — рациональное отображение плоских проективных кривых. Докажите, что ϕ определено над k в том и только том случае, когда $\sigma(\phi) = \phi$ для всех $\sigma \in \mathrm{Gal}(\bar{k}/k)$.

Подсказка: воспользуйтесь теоремой Гильберта 90.

Задача 10 (гиперэллиптические кривые). Пусть C_0 — аффинная кривая, заданная уравнением $y^d = a_0x^d + a_1x^{d-1} + \cdots + a_d$, над полем характеристики $\neq 2$, $a_0 \neq 0$.

a) Покажите, что точка на бесконечности у C_0 является особой тогда и только тогда, когда $d \geq 4$.

b) Пусть $d = 4$. Рассмотрим отображение $\psi = [1, x, y, x^2]\colon C_0 \to \mathbb{P}^3$. Пусть C — кривая в $\mathbb{P}^3$, заданная уравнениями $x_2^2 - a_0x_3^2 - a_1x_1x_3 - a_2x_0x_3 - a_3x_0x_1 - a_4x_0^2 = x_3x_0 - x_1^2 = 0$. Убедитесь, что ψ задает изоморфизм $C_0 \cong C \cap \{x_0 \neq 0\}$.

c) Покажите, что кривая C имеет две неособые точки на пересечении с плоскостью $x_0 = 0$.

d^*) Обобщите предыдущее на произвольное $d \geq 4$.

Задача 11 (приведение эллиптических кривых к каноническому виду). a) Пусть E/k — неособая проективная кубическая кривая, $O \in E(k)$ — точка перегиба. Покажите, что найдется обратимая проективная линейная замена координат, переводящая O в $[0,1,0]$, а касательную к C в O в прямую $z = 0$.

b) Покажите, что, если кривая имеет вид, указанный в предыдущем пункте, то ее уравнение есть $y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$.

c) Пусть E/k — неособая проективная кубическая кривая, $O \in E(k)$ — точка, *не являющаяся* точкой перегиба. Можно считать, что касательная к E в точке O есть ось y, пересекающая E во второй точке $P = [0,0,1] \neq O$. В таком случае уравнение E имеет вид $F_1(x,y)z^2 + F_2(x,y)z + F_3(x,y) = 0$, где F_i — однородные степени i. Пусть C — кривая, заданная уравнением $s^2 = F_2(1,t)^2 - 4F_1(1,t)F_3(1,t)$. Докажите, что отображение $(s,t) \mapsto (2F_3(1,y/x)x + F_2(1,y/x), y/x)$ из $k[s,t]$ в $k[x,y][x^{-1}]$ продолжается до изоморфизма E и C, переводящего O в точку перегиба $[0,1,0]$.

Задача 12 (эллиптические кривые над полем произвольной характеристики). Пусть кривая E задана уравнением Вейерштрасса $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Введем обозначения:

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2;$$
$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6;$$
$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \quad j = \frac{c_4^3}{\Delta}.$$

a) Покажите, что линейной заменой переменных над полем k характеристики $\neq 2$ уравнение приводится к виду $y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$, а над полем характеристики $\neq 2, 3$ к виду $y^2 = x^3 - 27c_4x - 54c_6$.

b) Покажите, что для кривой вида $y^2 = x^3 + ax + b$ формулы для Δ и j упрощаются и принимают вид: $\Delta = -16 \cdot (4a^3 + 27b^2)$, $j = -1728 \cdot (4a)^3/\Delta$.

c) Докажите, что кривая E гладкая в том и только том случае, когда $\Delta \neq 0$.

d) Если $\Delta = 0$, то кривая имеет узел (“node”, особая точка с различными касательными) при $c_4 \neq 0$ и точку возврата (“cusp”, особая точка с совпадающими касательными) иначе.

e) Убедитесь, что единственные замены переменных, переводящие в уравнение Вейерштрасса (гладкой) эллиптической кривой в уравнение Вейерштраса, имеют следующий вид: $x = u^2x' + r$, $y = u^3y' + u^2sx' + t$.

f) Выведите формулы для преобразования коэффициентов:

$$ua_1' = a_1 + 2s, \quad u^2a_2' = a_2 - sa_1 + 3r - s^2,$$
$$u^3a_3' = a_3 + ra_1 + 2t, \quad u^4a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st,$$
$$u^6a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1;$$
$$u^2b_2' = b_2 + 12r, \quad u^4b_4' = b_4 + rb_2 + 6r^2,$$
$$u^6b_6' = b_6 + 2rb_4 + r^2b_2 + 4r^3, \quad u^8b_8' = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4;$$
$$u^4c_4' = c_4, \quad u^6c_6' = c_6, \quad u^{12}\Delta' = \Delta, \quad j' = j.$$

g) Покажите, что эллиптические кривые E и E' изоморфны над $\bar{k}$ тогда и только тогда, когда $j(E) = j(E')$.

h) Убедитесь, что для $j_0 \neq 0, 1728$ кривая $y^2+xy = x^3-\frac{36}{j_0-1728}x-\frac{1}{j_0-1728}$ имеет j-инвариант, равный j_0. Какие j-инварианты имеют кривые $y^2 + y = x^3$ и $y^2 = x^3 + x$?

i) Пусть $P_i = (x_i, y_i)$, $P_3 = P_1 + P_2$. Выведите следующие формулы для сложения точек на эллиптической кривой:

$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3),$$
$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \quad \text{при } x_1 \neq x_2,$$
$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \quad \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \quad \text{при } x_1 = x_2,$$
$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \quad y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

Задача 13°. Вычислите дискриминанты и j-инварианты следующих эллиптических кривых. Приведите их к виду $y^2 = x^2 + ax + b$ над полем характеристики $\neq 2, 3$.
a) $y^2 + y = x^3 - x^2$; b) $y^2 + y = x^3 + x^2$; c) $y^2 + y = x^3 - x$; d) $y^2 + y = x^3 + x$;
e) $y^2 - yx + y = x^3$; f) $y^2 - y = x^3 - 7$; g) $y^2 = x^3 + x^2 - x$; h) $y^2 = x^3 + x^2 + x$;
i) $y^2 = x^3 - 2x^2 - x$; j) $y^2 = x^3 - x^2 - 15x$.

Задача 14 (особые кубики). Пусть E/k — особая кубика в форме Вейерштрасса. Обозначим через E_{ns} множество неособых точек E.

a) Покажите, что E_{ns} является группой при стандартном определении операции с помощью касательных и секущих.

b) Пусть E имеет особую точку типа node и касательные $y = \alpha_i x + \beta_i$ в ней. Убедитесь, что, если $\alpha_1 \in k$, то $\alpha_2 \in k$ и $E_{ns}(k) \cong k^\times$.

c) В предположениях предыдущего пункта допустим, что $\alpha_1 \notin k$. Убедитесь, что $L = k(\alpha_1, \alpha_2)$ — квадратичное расширение k, $E_{ns}(L) \cong L^\times$ и $E_{ns}(k) \cong \{t \in L^\times \mid N_{L/k}(t) = 1\}$.

d) Пусть E имеет особую точку типа cusp. Покажите, что $E_{ns}(k) \cong k^+$ (поле k как группа по сложению).

Подсказка: в случае алгебраически замкнутого поля k можно воспользоваться отображениями $(x, y) \mapsto \frac{y-\alpha_1x-\beta_1}{y-\alpha_2x-\beta_2}$ для node'а и $(x, y) \mapsto \frac{x-x_0}{y-\alpha x-\beta}$ для cusp'а (x_0 — это x-координата особой точки, а $y = \alpha x+\beta$ — касательная в ней). Для упрощения вычислений особую точку можно перенести в $(0, 0)$.

Задача 15. Покажите, что отбражения $+\colon E \times E \to E$, $(P_1, P_2) \mapsto P_1 + P_2$ и $-\colon E \to E$, $P \mapsto -P$ являются регулярными морфизмами проективных многообразий.

Подсказка: "+", очевидно, является морфизмом вне точек вида (P,P), $(P,-P)$, (P,O), (O,P). Такие точки можно "немного подвинуть", а можно поработать руками с формулами.

Задача 16 (группа автоморфизмов). Пусть E/k — эллиптическая кривая, а $\mathrm{Aut}(E) = \mathrm{Aut}_{\bar{k}}(E)$ — группа ее $\bar{k}$-автоморфизмов. Покажите, что

a) Если $j(E) \neq 0, 1728$, то $\mathrm{Aut}(E) \cong \mathbb{Z}/2\mathbb{Z}$.

b) Пусть $\operatorname{char} k \neq 2, 3$. Тогда $\mathrm{Aut}(E) \cong \mathbb{Z}/4\mathbb{Z}$, если $j(E) = 1728$, и $\mathrm{Aut}(E) \cong \mathbb{Z}/6\mathbb{Z}$, если $j(E) = 0$.

c) Пусть $\operatorname{char} k = 3$, а $j(E) = 0 = 1728$. Тогда $\mathrm{Aut}(E) \cong \mathbb{Z}/3\mathbb{Z} \leftthreetimes \mathbb{Z}/4\mathbb{Z}$ (полупрямое произведение, в котором образующая $\mathbb{Z}/4\mathbb{Z}$ действует нетривиально на нормальную подгруппу $\mathbb{Z}/3\mathbb{Z}$, переводя каждый элемент в обратный ему).

d) Пусть $\operatorname{char} k = 2$, а $j(E) = 0 = 1728$. Тогда $\mathrm{Aut}(E) \cong SL_2(\mathbb{F}_3)$.

Задача 17 (эллиптические кривые над конечным полем).

a) Опишите все неизоморфные эллиптические кривые над полем $\mathbb{F}_2$. Какие у них j-инварианты?
Подсказка: чтобы показать, что кривые не изоморфны, можно посмотреть на количество точек на них.

b) Какие из полученных в предыдущем пункте кривых становятся изомофными над $\mathbb{F}_4$? Над $\mathbb{F}_{16}$? А над $\mathbb{F}_{256}$?

c) Посчитайте группы автоморфизмов кривых из предыдущего пункта над полями $\mathbb{F}_{2^k}$, $k \in \mathbb{N}$.

d) Опишите все различные (т. е. неизоморфные) кривые над $\mathbb{F}_4$. Какие у них j-инварианты? Какие из них становятся изоморфными над $\mathbb{F}_{16}$?

e) Аналогичных вопрос про кривые над $\mathbb{F}_3$ и $\mathbb{F}_5$. Опишите группы точек получившихся кривых.

Задача 18°. Пусть $\operatorname{char} k \neq 3$, $a \in k^\times$. Рассмотрим кривую $x^3 + y^3 = az^3$.

a) Покажите, что данная кривая является эллиптической и ее j-инвариант равен 0.

b) Выведите формулы для суммы точек на этой кривой.

Задача 19 (точки порядка 3). a°) Найдите необходимое и достаточное условие того, чтобы прямая $L\colon y = cx + d$ была касательной в точке перегиба к кривой $E\colon y^2 = x^3 + ax + b$ (т. е. $I(P, E \cap L) = 3$ в точке пересечения L с E).

b°) Получите описание эллиптических кривых в форма Вейерштрасса, имеющих рациональную точку порядка 3.

c) Покажите, что над $\bar{k}$, $\operatorname{char} k \neq 2, 3$ множество точек порядка 3 на эллиптической кривой состоит из 9 различных точек. Из скольких точек состоит множество точек порядка 2?

Задача 20 (умножение на m). Пусть $\operatorname{char} k \neq 2, 3$, E/k — кривая, заданная уравнением $y^2 = x^3 + ax + b$. Определим многочлены деления $\psi_m \in \mathbb{Z}[a, b, x, y]$ следующими формулами:

$$\psi_1 = 1, \quad \psi_2 = 2y, \quad , \psi_3 = 3x^4 + 6ax^2 + 12bx - a^2,$$
$$\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),$$
$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad (m \geq 2),$$
$$2y\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \quad (m \geq 3).$$

Кроме того, положим $\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}$ и $4y\omega_m = \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2$.

a) Покажите, что ψ_m, ϕ_m, $y^{-1}\omega_m$ (m — нечетно) и $(2y)^{-1}\psi_m$, ϕ_m, ω_m (m — четно) являются многочленами с коэффициентами из $\mathbb{Z}[a, b, x, y^2]$. Таким образом, заменив y^2 на $x^3 + ax + b$, можно считать, что мы имеем дело с многочленами из $\mathbb{Z}[a, b, x]$.

b) Покажите, что, рассматриваемые как многочлены от x, ϕ_m и ψ_m имеют разложения $\phi_m(x) = x^{m^2}$ + члены меньшего порядка, $\psi_m(x) = m^2x^{m^2-1}$ + члены меньшего порядка.

c) Если E неособа, то $\phi_m(x)$ и $\psi_m(x)^2$ взаимно просты как многочлены из $k[x]$.

d) Если E неособа и $P = (x_0, y_0) \in E$, то $[m]P = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3}\right)$ (здесь $[m]$ обозначает умножение на m на эллиптической кривой: $P + P + \cdots + P$ — m раз).

e) Покажите, что отображение умножения $[m] : E \to E$ имеет степень m^2.

Задача 21° (уравнение кривой в форме Лежандра). Пусть $\mathrm{char}\, k \neq 2$.

a) Покажите, что любая эллиптическая кривая E/k изоморфна над $\bar{k}$ эллиптической кривой в форме Лежандра $E_\lambda\colon y^2 = x(x-1)(x-\lambda)$, $\lambda \in \bar{k}, \lambda \neq 0, 1$.

b) Покажите, что $j(E_\lambda) = 2^8 \cdot \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$.

c) Убедитесь, что отображение $\bar{k} \setminus \{0, 1\} \to \bar{k}$, $\lambda \mapsto j(E_\lambda)$ имеет 6 пробразов во всех точках, кроме $j = 0$ и $j = 1728$. Сколько прообразов оно имеет в исключительных точках?

Задача 22° (уравнение кривой в форме Дойринга).

a) Пусть E/k — эллиптическая кривая и, либо $\mathrm{char}\, k \neq 3$, либо $j(E) \neq 0$. Покажите, что над $\bar{k}$ кривая E имеет уравнение Вейерштрасса вида $y^2 + \alpha xy + y = x^3$, $\alpha \in \bar{k}$.

b) Покажите, что для кривой E, заданной уравнением из предыдущего пункта $[3](0,0) = O$ (т. е. $(0,0)$ — точка порядка 3).

c) При каких α кривая неособая? Покажите, что $j(E) = \frac{\alpha^3(\alpha^3-24)^3}{\alpha^3-27}$.

Задача 23°. Пусть a, b, c, d — целые числа, свободные от квадратов, $a > b > c > 0$. Рассмотрим кривую в $\mathbb{P}^2$, заданную уравнением $C\colon ax^3 + by^3 + cz^3 + dxyz = 0$.

a) Пусть $P = [x, y, z] \in C$, L — касательная к C в P. Покажите, что $C \cap L = \{P, P'\}$. Вычислите $P' = [x', y', z']$ через a, b, c, d, x, y, z.

b) Покажите, что, если $P \in C(\mathbb{Q})$, то $P' \in C(\mathbb{Q})$.

c) Предположим, что $x, y, z, x', y', z' \in \mathbb{Z}$ и $\gcd(x, y, z) = \gcd(x', y', z') = 1$. Докажите, что $|x'y'z'| > |xyz|$.

d) Выведите из предыдущего пункта, что, либо $C(\mathbb{Q}) = \emptyset$, либо $C(\mathbb{Q})$ — бесконечное множество.

Задача 24 (кривые рода 1). Пусть $C/\bar{k}$ — кривая рода 1, $\mathrm{char}\, k \neq 2$. Каждой точке $O \in C$ можно сопоставить эллиптическую кривую (C, O) и ее j-инвариант $j(C, O)$. Наша цель — показать, что $j(C, O)$ не зависит от выбора O, а значит j-инвариант определен для любой кривой рода 1.

a) Выберем уравнение Лежандра $y^2 = x(x-1)(x-\lambda)$ для кривой (C, O). Покажите, что отображение $x\colon C \to \mathbb{P}^1$ имеет степень 2, причем для всех точек, отличных от 0, 1, λ, ∞, число прообразов равно двум.

b) Пусть $O' \in C$ — другая точка, а $w^2 = z(z-1)(z-\mu)$ — уравнение Лежандра для (C, O'). Пусть $\tau : C \to C$ перенос на O' на эллиптической кривой (C, O) (т. е. $\tau(P) = P + O'$). Докажите, что найдутся такие $a \in \bar{k}$, $b \in \bar{k}^\times$, что $\tau^*(z) = a + bx$ (как функции на C).
Подсказка: Посмотрите на дивизор $\tau^*(z)$.

c) Пусть $f : \mathbb{P}^1 \to \mathbb{P}^1$, $f(t) = a + bt$. Покажите, что f — биективно отображает множество $\{0, 1, \lambda\}$ на $\{0, 1, \mu\}$.

d) Покажите, что $\mu \in \{\lambda, 1/\lambda, 1-\lambda, 1/(1-\lambda), \lambda/(1-\lambda), (\lambda-1)/\lambda\}$.

e) Убедитесь, что $j(C, O) = j(C, O')$.

f) Пусть C — кривая рода 1, определенная над k. Покажите, что $j(C) \in k$.

g) Докажите, что C/k изоморфна над $\bar{k}$ эллиптической кривой, определенной над k.

h^*) Докажите аналогичные результаты над полем k характеристики 2.

Задача 25 (эллиптические кривые в пространстве). Пусть E/k — эллиптическая кривая, заданная уравнением Вейерштрасса.

a) Покажите, что $\phi : E \to \mathbb{P}^3$, $\phi = [1, x, y, x^2]$ изоморфно отображает E на пересечение квадратичных поверхностей в $\mathbb{P}^3$.

b) Выведите из этого, что, если $H \subset \mathbb{P}^3$ — плоскость, то $H \cap \phi(E)$ состоит из 4 точек (считая кратности). Убедитесь, что $\phi(O) = [0, 0, 0, 1]$ и плоскость $T_0 = 0$ пересекает $\phi(E)$ в единственной точке $\phi(O)$ с кратностью 4.

c) Пусть $P, Q, R \in E$. Докажите, что $P + Q + R = O$ тогда и только тогда, когда $\phi(P)$, $\phi(Q)$, $\phi(R)$, $\phi(O)$ лежат в одной плоскости.

d) Пусть $P \in E$. Покажите, что $[4]P = O$ тогда и только тогда, когда существует такая плоскость $H \subset \mathbb{P}^3$, что $H \cap \phi(E) = P$.

e) Покажите, что, если $\operatorname{char} k \neq 2$, то имеется ровно 16 таких точек, что $[4]P = O$.

f) Пусть $\operatorname{char} k \neq 2$. Покажите, что существует линейная замена переменных над $\bar{k}$, приводящая уравнения E в $\mathbb{P}^3$ к виду $T_0^2 + T_2^2 = T_0T_3$, $T_1^2 + \alpha T_2^2 = T_2T_3$. Для каких α данная кривая неособая?

g) Используя модель из предыдущего пункта, выведите явные формулы для $-P$, $P_1 + P_2$ и $[2]P$ (в координатах в $\mathbb{P}^3$).

h^*) Обобщите задачу на случай вложения E в $\mathbb{P}^m$, определенного функциями $f_1, \ldots, f_m$, образующими базис в $L(m[O])$.